PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-134264**

(43)Date of publication of application : **20.05.1997**

(51)Int.Cl.

G06F 3/12
B41J 5/30
B41J 29/38
G06F 13/00
G09C 1/00
H04L 9/30

(21)Application number : **07-289525**

(22)Date of filing : **08.11.1995**

(71)Applicant : **CANON INC**

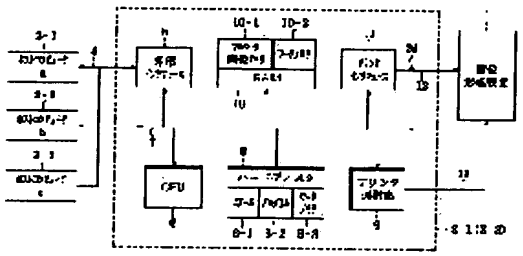
(72)Inventor : **KADOWAKI TOSHIHIRO**

(54) PICTURE PROCESSOR, INFORMATION PROCESSOR, PICTURE PROCESSING SYSTEM AND JOB PROCESSING METHOD FOR PICTURE PROCESSING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a print job processing environment where a print job on a communication medium can easily be ciphered, the ciphered print job cannot practically be decoded by a device except for a picture processor and security protection is superior.

SOLUTION: When an external interface 5 receives the print job ciphered by ciphered key information from respective computers 2-1 and 2-2 after ciphered key information for ciphering the print job by the external interface 5 is reported the respective computers 2-1 and 2-2, CPU 6 decodes the received and ciphered print job based on decoding key information stored in a work memory area 8-3. CPU 6 develops picture data on respective pages in the print job which CPU 6 decodes on a full page picture memory 10-1.



LEGAL STATUS

[Date of request for examination] 30.06.1998

[Date of sending the examiner's decision of rejection]	30.10.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3281235
[Date of registration]	22.02.2002
[Number of appeal against examiner's decision of rejection]	2001-021228
[Date of requesting appeal against examiner's decision of rejection]	29.11.2001
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－134264

(43)公開日　平成９年(1997)５月20日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　3/12			Ｇ０６Ｆ　3/12	Ｄ	
				Ｋ	
Ｂ４１Ｊ　5/30			Ｂ４１Ｊ　5/30	Ｚ	
29/38			29/38	Ｚ	
Ｇ０６Ｆ　13/00	３５１		Ｇ０６Ｆ　13/00	３５１Ｇ	

審査請求　未請求　請求項の数28　ＯＬ　（全 26 頁）　最終頁に続く

(21)出願番号　特願平7－289525

(22)出願日　平成７年(1995)11月８日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　門脇　俊浩
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

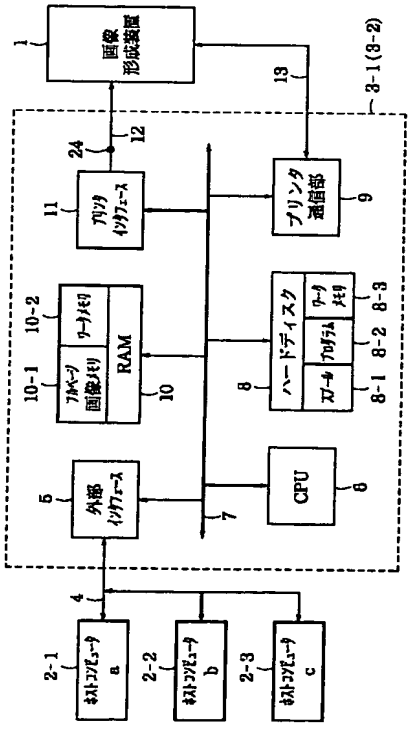
(74)代理人　弁理士　小林　将高

(54)【発明の名称】　画像処理装置並びに情報処理装置並びに画像処理システムおよび画像処理システムのジョブ処理方法

(57)【要約】

【課題】　通信媒体上のプリントジョブを容易に暗号化し、かつ、画像処理装置以外は暗号化されたプリントジョブを実質上復号化できない機密保持性に優れたプリントジョブ処理環境を構築することである。

【解決手段】　外部インタフェース５による前記プリントジョブを暗号化するための暗号化鍵情報を各コンピュータ２－１，２－２に通知後、外部インタフェース５が前記暗号化鍵情報により暗号化されたプリントジョブを各コンピュータ２－１，２－２から受信したら、ＣＰＵ６が受信した暗号化されたプリントジョブをワークメモリ領域８－３に記憶された前記復号化鍵情報に基づいて復号化し、ＣＰＵ６が該復号化したプリントジョブ中の各ページの画像データをフルページ画像メモリ１０－１上に展開する構成を特徴とする。



【特許請求の範囲】

【請求項１】　所定の通信媒体を介して複数の情報処理装置から受信したプリントジョブに基づいて画像処理を行う画像処理装置において、前記プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知する通知手段と、前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信するプリントジョブ受信手段と、前記暗号化鍵情報に対応した復号化鍵情報を記憶する記憶手段と、受信したプリントジョブを前記復号化鍵情報に基づいて復号化する復号手段と、画像データを記憶する画像メモリ手段と、復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開する展開手段とを具備したことを特徴とする画像処理装置。

【請求項２】　前記通知手段は、同一の暗号化鍵情報を前記通信媒体を介して各情報処理装置に通知することを特徴とする請求項１記載の画像処理装置。

【請求項３】　前記通信媒体は、所定のネットワークであることを特徴とする請求項２記載の画像処理装置。

【請求項４】　前記復号手段は、前記展開手段による画像データの展開の直前、もしくは展開中に前記受信したプリントジョブの復号を行うことを特徴とする請求項１記載の画像処理装置。

【請求項５】　前記暗号化鍵情報に対する前記復号化鍵情報との組合せを複数備えることを特徴とする請求項１記載の画像処理装置。

【請求項６】　前記プリントジョブに付加された有効期限情報に基づいて受信したプリントジョブの処理を制御する第１の制御手段を有することを特徴とする請求項１記載の画像処理装置。

【請求項７】　前記有効期限情報は、暗号化された状態で前記プリントジョブに付加されていることを特徴とする請求項１記載の画像処理装置。

【請求項８】　受信したプリントジョブを作成した情報処理装置と受信したプリントジョブを送信した情報処理装置とが同一であるか認証する認証手段と、前記認証手段の認証結果に基づいて受信したプリントジョブの処理を制御する第２の制御手段とを有することを特徴とする請求項１記載の画像処理装置。

【請求項９】　前記プリントジョブ受信手段は、前記暗号化鍵情報により暗号化されたプリントジョブおよび暗号化鍵情報を併せて各情報処理装置から受信することを特徴とする請求項１記載の画像処理装置。

【請求項１０】　プリントジョブ受信手段が各情報処理装置から受信する暗号化鍵情報は暗号化されていない状態で受信することを特徴とする請求項１記載の画像処理装置。

【請求項１１】　前記暗号化鍵情報により暗号化されたプリントジョブを印刷候補として複数一時的に保持する第１の保持手段を有することを特徴とする請求項１記載の画像処理装置。

【請求項１２】　前記暗号化鍵情報により暗号化されたプリントジョブを出力待機候補として複数一時的にそのまま保持する第２の保持手段を有することを特徴とする請求項１記載の画像処理装置。

【請求項１３】　前記展開手段により画像メモリ上に展開された画像データを画像出力装置に送出する送出手段と、前記送出手段により前記画像出力装置に送出されて画像出力が完了した前記暗号化鍵情報により暗号化されたプリントジョブを破棄候補として複数一時的に保持する第３の保持手段を有することを特徴とする請求項１記載の画像処理装置。

【請求項１４】　前記展開手段により画像メモリ上に展開された画像データを画像出力装置に送出する送出手段と、前記送出手段により前記画像出力装置に送出されて画像出力が完了した前記暗号化鍵情報により暗号化されていないプリントジョブを破棄候補として複数一時的に保持する第３の保持手段を有することを特徴とする請求項１記載の画像処理装置。

【請求項１５】　前記暗号化されたプリントジョブは、所定のページ記述言語で記述された印刷情報を暗号化鍵情報に基づいて暗号化したものであることを特徴とする請求項１，４，６～９，１１～１４のいずれかに記載の画像処理装置。

【請求項１６】　前記暗号化鍵情報と対となる復号化鍵情報は、所定の公開鍵暗号方式に準拠することを特徴とする請求項１記載の画像処理装置。

【請求項１７】　所定の通信媒体を介して複数の画像処理装置と通信可能な情報処理装置において、いずれかの画像処理装置から所定の暗号化鍵情報を受信する暗号受信手段と、前記暗号受信手段により受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化する暗号化手段と、前記暗号化手段により暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置に送信するプリントジョブ送信手段とを有することを特徴とする情報処理装置。

【請求項１８】　前記暗号受信手段により前記所定の通信媒体を介して各画像処理装置から受信した固有の暗号化鍵情報を記憶する第１の暗号化鍵情報記憶手段を設けたことを特徴とする請求項１７記載の情報処理装置。

【請求項１９】　前記暗号受信手段は、前記暗号化手段による暗号化開始直前に各画像処理装置から前記固有の暗号化鍵情報を受信することを特徴とする請求項１７記載の情報処理装置。

【請求項２０】　前記暗号受信手段により前記所定の通信媒体を介して各画像処理装置から受信した複数の画像処理装置で共通する暗号化鍵情報を記憶する第２の暗号化鍵情報記憶手段を設けたことを特徴とする請求項１７記載の情報処理装置。

【請求項２１】　前記暗号受信手段は、前記暗号化手段

による暗号化開始直前に複数の画像処理装置で共通する暗号化鍵情報を受信することを特徴とする請求項１７記載の情報処理装置。

【請求項２２】　前記プリントジョブは、画像処理装置における画像処理実行状態を制御するための所定の有効期限情報を含むことを特徴とする請求項１７記載の情報処理装置。

【請求項２３】　前記暗号化手段は、画像処理装置における画像処理実行状態を制御するための所定の有効期限情報を含むプリントジョブを暗号化することを特徴とする請求項１７記載の情報処理装置。

【請求項２４】　前記プリントジョブ送信手段は、前記暗号化手段により暗号化されたプリントジョブおよび前記暗号化手段が暗号化に使用した前記所定の暗号化鍵情報も同時に画像処理装置に送信することを特徴とする請求項１７記載の情報処理装置。

【請求項２５】　前記プリントジョブ送信手段は、前記暗号化手段が暗号化に使用した前記所定の暗号化鍵情報をそのまま画像処理装置に送信することを特徴とする請求項２４記載の情報処理装置。

【請求項２６】　所定の通信媒体を介して複数の画像処理装置と複数の情報処理装置とが通信可能な画像処理システムにおいて、いずれかの画像処理装置から所定の暗号化鍵情報を受信する暗号受信手段と、前記暗号受信手段により受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化する暗号化手段と、前記暗号化手段により暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置に送信するプリントジョブ送信手段とを有する情報処理装置と、所定の通信媒体を介して複数の情報処理装置から受信したプリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知する通知手段、前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信するプリントジョブ受信手段、前記暗号化鍵情報に対応した復号化鍵情報を記憶する記憶手段と、受信したプリントジョブを前記復号化鍵情報に基づいて復号化する復号手段、画像データを記憶する画像メモリ手段と、復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開する展開手段とを有する画像処理装置とを備えることを特徴とする画像処理システム。

【請求項２７】　所定の通信媒体を介して複数の画像処理装置と複数の情報処理装置とが通信可能な画像処理システムのジョブ処理方法において、いずれかの画像処理装置から所定の暗号化鍵情報を受信する暗号受信工程と、該受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化する暗号化工程と、該暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置にプリントジョブ送信する送信工程とを有する画像処理システムのジョブ処理方法。

【請求項２８】　所定の通信媒体を介して複数の画像処理装置と複数の情報処理装置とが通信可能な画像処理システムのジョブ処理方法において、所定の通信媒体を介して複数の情報処理装置から受信したプリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知する通知工程、前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信するプリントジョブ受信工程、受信したプリントジョブを前記復号化鍵情報に基づいて復号化する復号工程と、該復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開する展開工程とを有することを特徴とする画像処理システムのジョブ処理方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、所定の通信媒体を介して所定のページ記述言語（Page DescriptionLanguage：以下ＰＤＬという）で記述されたＰＤＬデータを処理する画像処理装置並びに情報処理装置並びに画像処理システムおよび画像処理システムのジョブ処理方法に関するものである。

【０００２】

【従来の技術】従来、ホストコンピュータ等から、ＰＤＬデータにより構成されるプリントジョブをネットワーク経由で受信し、該プリントジョブを処理し、プリンタに送って画像を形成する画像処理装置では、特に暗号化を施していない形でプリントジョブを受信していた。

【０００３】

【発明が解決しようとする課題】このように上記従来の画像処理装置においては、ホストコンピュータから送られてきたプリントジョブは、暗号化を施していないため、以下のような問題があった。

【０００４】１）特に、複数のホストコンピュータと複数の画像処理装置がネットワークで接続されている場合、他のホストコンピュータ等によりプリントデータを盗まれたり、中身を見られる可能性があった。

【０００５】また、ネットワーク上の信号を観測することによりプリントデータを盗まれたり、中身を見られる可能性があった。

【０００６】２）通常、ＰＤＬデータは可読性を良くするため、人間が読むことのできるアスキーデータで構成されている場合があり、この場合はさらにセキュリティが悪化する。

【０００７】本発明は、上記の問題点を解消するためになされたもので、本発明に係る第１の発明～第２８の発明の目的は、画像処理装置が装置固有あるいは複数の装置で共通する暗号化鍵を複数の情報処理装置に公開し、各情報処理装置がプリントジョブを公開された暗号化鍵を用いて暗号化しつつ画像処理装置に送信することにより、通信媒体上のプリントジョブを容易に暗号化し、か

つ、画像処理装置以外は暗号化されたプリントジョブを実質上復号化でいない機密保持性に優れたプリントジョブ処理環境を構築できる画像処理装置並びに情報処理装置並びに画像処理システムおよび画像処理システムのジョブ処理方法を提供することである。

【０００８】

【課題を解決するための手段】本発明に係る第１の発明は、所定の通信媒体を介して複数の情報処理装置から受信したプリントジョブに基づいて画像処理を行う画像処理装置において、前記プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知する通知手段と、前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信するプリントジョブ受信手段と、前記暗号化鍵情報に対応した復号化鍵情報を記憶する記憶手段と、受信したプリントジョブを前記復号化鍵情報に基づいて復号化する復号手段と、画像データを記憶する画像メモリ手段と、復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開する展開手段とを設けたものである。

【０００９】本発明に係る第２の発明は、前記通知手段は、同一の暗号化鍵情報を前記通信媒体を介して各情報処理装置に通知するものである。

【００１０】本発明に係る第３の発明は、前記通信媒体は、所定のネットワークであるものである。

【００１１】本発明に係る第４の発明は、前記復号手段は、前記展開手段による画像データの展開の直前、もしくは展開中に前記受信したプリントジョブの復号を行うものである。

【００１２】本発明に係る第５の発明は、前記暗号化鍵情報に対する前記復号化鍵情報との組合せを複数備えるものである。

【００１３】本発明に係る第６の発明は、前記プリントジョブに付加された有効期限情報に基づいて受信したプリントジョブの処理を制御する第１の制御手段を有するものである。

【００１４】本発明に係る第７の発明は、前記有効期限情報は、暗号化された状態で前記プリントジョブに付加されているものである。

【００１５】本発明に係る第８の発明は、受信したプリントジョブを作成した情報処理装置と受信したプリントジョブを送信した情報処理装置とが同一であるか認証する認証手段と、前記認証手段の認証結果に基づいて受信したプリントジョブの処理を制御する第２の制御手段とを有するものである。

【００１６】本発明に係る第９の発明は、前記プリントジョブ受信手段は、前記暗号化鍵情報により暗号化されたプリントジョブおよび暗号化鍵情報を併せて各情報処理装置から受信するものである。

【００１７】本発明に係る第１０の発明は、プリントジョブ受信手段が各情報処理装置から受信する暗号化鍵情報は暗号化されていない状態で受信するものである。

【００１８】本発明に係る第１１の発明は、前記暗号化鍵情報により暗号化されたプリントジョブを印刷候補として複数一時的に保持する第１の保持手段を有するものである。

【００１９】本発明に係る第１２の発明は、前記暗号化鍵情報により暗号化されたプリントジョブを出力待機候補として複数一時的にそのまま保持する第２の保持手段を有するものである。

【００２０】本発明に係る第１３の発明は、前記展開手段により画像メモリ上に展開された画像データを画像出力装置に送出する送出手段と、前記送出手段により前記画像出力装置に送出されて画像出力が完了した前記暗号化鍵情報により暗号化されたプリントジョブを破棄候補として複数一時的に保持する第３の保持手段を有するものである。

【００２１】本発明に係る第１４の発明は、前記展開手段により画像メモリ上に展開された画像データを画像出力装置に送出する送出手段と、前記送出手段により前記画像出力装置に送出されて画像出力が完了した前記暗号化鍵情報により暗号化されていないプリントジョブを破棄候補として複数一時的に保持する第３の保持手段を有するものである。

【００２２】本発明に係る第１５の発明は、前記暗号化されたプリントジョブは、所定のページ記述言語で記述された印刷情報を暗号化鍵情報に基づいて暗号化したものであるものである。

【００２３】本発明に係る第１６の発明は、前記暗号化鍵情報と対となる復号化鍵情報は、所定の公開鍵暗号方式に準拠するものである。

【００２４】本発明に係る第１７の発明は、所定の通信媒体を介して複数の画像処理装置と通信可能な情報処理装置において、いずれかの画像処理装置から所定の暗号化鍵情報を受信する暗号受信手段と、前記暗号受信手段により受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化する暗号化手段と、前記暗号化手段により暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置に送信するプリントジョブ送信手段とを有するものである。

【００２５】本発明に係る第１８の発明は、前記暗号受信手段により前記所定の通信媒体を介して各画像処理装置から受信した固有の暗号化鍵情報を記憶する第１の暗号化鍵情報記憶手段を設けたものである。

【００２６】本発明に係る第１９の発明は、前記暗号受信手段は、前記暗号化手段による暗号化開始直前に各画像処理装置から前記固有の暗号化鍵情報を受信するものである。

【００２７】本発明に係る第２０の発明は、前記暗号受信手段により前記所定の通信媒体を介して各画像処理装

置から受信した複数の画像処理装置で共通する暗号化鍵情報を記憶する第２の暗号化鍵情報記憶手段を設けたものである。

【００２８】本発明に係る第２１の発明は、前記暗号受信手段は、前記暗号化手段による暗号化開始直前に複数の画像処理装置で共通する暗号化鍵情報を受信するものである。

【００２９】本発明に係る第２２の発明は、前記プリントジョブは、画像処理装置における画像処理実行状態を制御するための所定の有効期限情報を含むものである。

【００３０】本発明に係る第２３の発明は、前記暗号化手段は、画像処理装置における画像処理実行状態を制御するための所定の有効期限情報を含むプリントジョブを暗号化するものである。

【００３１】本発明に係る第２４の発明は、前記プリントジョブ送信手段は、前記暗号化手段により暗号化されたプリントジョブおよび前記暗号化手段が暗号化に使用した前記所定の暗号化鍵情報も同時に画像処理装置に送信するものである。

【００３２】本発明に係る第２５の発明は、前記プリントジョブ送信手段は、前記暗号化手段が暗号化に使用した前記所定の暗号化鍵情報をそのまま画像処理装置に送信するものである。

【００３３】本発明に係る第２６の発明は、所定の通信媒体を介して複数の画像処理装置と複数の情報処理装置とが通信可能な画像処理システムにおいて、いずれかの画像処理装置から所定の暗号化鍵情報を受信する暗号受信手段と、前記暗号受信手段により受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化する暗号化手段と、前記暗号化手段により暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置に送信するプリントジョブ送信手段とを有する情報処理装置と、所定の通信媒体を介して複数の情報処理装置から受信したプリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知する通知手段、前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信するプリントジョブ受信手段、前記暗号化鍵情報に対応した復号化鍵情報を記憶する記憶手段と、受信したプリントジョブを前記復号化鍵情報に基づいて復号化する復号手段、画像データを記憶する画像メモリ手段と、復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開する展開手段とを有するものである。

【００３４】本発明に係る第２７の発明は、所定の通信媒体を介して複数の画像処理装置と複数の情報処理装置とが通信可能な画像処理システムのジョブ処理方法において、いずれかの画像処理装置から所定の暗号化鍵情報を受信する暗号受信工程と、該受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化する暗号化工程と、該暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置にプリントジョブ送信する送信工程とを有するものである。

【００３５】本発明に係る第２８の発明は、所定の通信媒体を介して複数の画像処理装置と複数の情報処理装置とが通信可能な画像処理システムのジョブ処理方法において、プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知する通知工程、前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信するプリントジョブ受信工程、受信したプリントジョブを前記復号化鍵情報に基づいて復号化する復号工程と、該復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開する展開工程とを有するものである。

【００３６】

【作用】第１の発明においては、通知手段による前記プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知後、プリントジョブ受信手段が前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信したら、復号手段が受信した暗号化されたプリントジョブを前記記憶手段に記憶された前記復号化鍵情報に基づいて復号化し、展開手段が該復号化したプリントジョブ中の各ページの画像データを画像メモリ上に展開して、通信媒体上に出力された該プリントジョブは該暗号化鍵情報を提示した画像処理装置以外の画像処理装置では実質上復号化不能とした状態で転送し、該暗号化鍵情報を復号可能な画像処理装置の復号化鍵情報に基づいて画像出力可能なプリントジョブに復号してプリントジョブを処理することを可能とする。

【００３７】第２の発明においては、前記通知手段は、同一の暗号化鍵情報を前記通信媒体を介して各情報処理装置に通知して、プリントジョブを暗号化するための暗号化鍵情報を全ての情報処理装置に対して共通化することを可能とする。

【００３８】第３の発明においては、所定のネットワークを介して暗号化鍵情報を複数の情報処理装置に通知して、各情報処理装置に通知した暗号化鍵情報を容易に変更可能とする。

【００３９】第４の発明においては、復号手段は、前記展開手段による画像データの展開の直前、もしくは展開中に前記受信した暗号化されたプリントジョブの復号を行い、暗号化されたプリントジョブ全体が復号化されてしまう事態を回避することを可能とする。

【００４０】第５の発明においては、暗号化鍵情報に対する前記復号化鍵情報との組合せを複数備え、他の画像処理装置と共有してあるいは各画像処理装置固有にプリントジョブを暗号化／復号化する異なる環境を共存させることを可能とする。

【００４１】第６の発明においては、第１の制御手段は前記プリントジョブに付加された有効期限情報に基づいて受信したプリントジョブの処理を制御して、暗号化さ

れたプリントジョブが転送中に第３者により入手されてしまっても、有効期限情報の制約に合致しない場合には、復号化できたプリントジョブであってもその画像出力を確実に制限することを可能とする。

【００４２】第７の発明においては、有効期限情報は、暗号化された状態で前記プリントジョブに付加して、有効期限情報の書き換えを防止することを可能とする。

【００４３】第８の発明においては、認証手段により受信したプリントジョブを作成した情報処理装置と受信したプリントジョブを送信した情報処理装置とが同一であるかを認証し、該認証結果に基づいて第２の制御手段が受信したプリントジョブの処理を制御して、いずれかの情報処理装置が通知された暗号化鍵情報に基づいて暗号化されたプリントジョブを他の情報処理装置が取得する事態が発生しても、該他の情報処理装置から取得したプリントジョブを対応する画像処理装置から出力されてしまう事態を確実に制限することを可能とする。

【００４４】第９の発明においては、プリントジョブ受信手段は、前記暗号化鍵情報により暗号化されたプリントジョブおよび暗号化鍵情報を併せて各情報処理装置から受信して、受信したプリントジョブの暗号化状態を確実に識別して、対応する最適な復号化鍵情報に基づいて受信したプリントジョブを正常に復号化することを可能とする。

【００４５】第１０の発明においては、プリントジョブ受信手段が各情報処理装置から受信する暗号化鍵情報は暗号化されていない状態で受信し、受信した暗号化鍵情報と通知した暗号化鍵情報とから暗号化に使用された暗号化鍵情報を確実に識別することを可能とする。

【００４６】第１１の発明においては、第１の保持手段が前記暗号化鍵情報により暗号化されたプリントジョブを印刷候補として複数一時的に保持して、印刷候補となるプリントジョブ自体は印刷される直前まで暗号化された状態で保持することを可能とする。

【００４７】第１２の発明においては、第２の保持手段が前記暗号化鍵情報により暗号化されたプリントジョブを出力待機候補として複数一時的にそのまま保持して、出力待機状態となっているプリントジョブ自体は印刷される直前まで暗号化された状態で保持することを可能とする。

【００４８】第１３の発明においては、前記展開手段により画像メモリ上に展開された画像データが送出手段により画像出力装置に送出されて、前記画像出力装置による画像出力が完了したら、第３の保持手段が前記暗号化鍵情報により暗号化されたプリントジョブを破棄候補として複数一時的に保持して、復号化されて画像出力装置から出力されてしまったプリントジョブがそのままの状態で保持されてしまうことを回避することを可能とする。

【００４９】第１４の発明においては、前記展開手段により画像メモリ上に展開された画像データが送出手段により画像出力装置に送出されて、前記画像出力装置による画像出力が完了したら、第３の保持手段が前記暗号化鍵情報により暗号化されていないプリントジョブを破棄候補として複数一時的に保持して、画像出力が完了している暗号化されていたプリントジョブが不用意に保持される状態を回避することを可能とする。

【００５０】第１５の発明においては、前記暗号化されたプリントジョブは、所定のページ記述言語で記述された印刷情報を暗号化鍵情報に基づいて暗号化して、ページ記述言語中で容易に可読できるデータを確実に暗号化して転送処理することを可能とする。

【００５１】第１６の発明においては、前記暗号化鍵情報と対となる復号化鍵情報は、所定の公開鍵暗号方式に準拠し、プリントジョブの暗号化／復号化処理環境を容易に構築することを可能とする。

【００５２】第１７の発明においては、暗号受信手段がいずれかの画像処理装置から所定の暗号化鍵情報を受信したら、該受信された前記所定の暗号化鍵情報に基づいて暗号化手段が作成されたプリントジョブを暗号化し、該暗号化されたプリントジョブをプリントジョブ送信手段が前記所定の暗号化鍵情報を受信した画像処理装置に送信して、いずれの情報処理装置に対しても同一の暗号化鍵情報で通知して暗号化されたプリントジョブの復号化処理を画一化することを可能とする。

【００５３】第１８の発明においては、第１の暗号化鍵情報記憶手段が前記暗号受信手段により前記所定の通信媒体を介して各画像処理装置から受信した固有の暗号化鍵情報を記憶して、いずれの画像処理装置に対しても対応する暗号化鍵情報に基づいて暗号化されたプリントジョブを転送可能とする。

【００５４】第１９の発明においては、暗号受信手段は、前記暗号化手段による暗号化開始直前に各画像処理装置から前記固有の暗号化鍵情報を受信して、各画像処理装置が通知する暗号化鍵情報が変更されても、常に復号可能となる最新の暗号化鍵情報に基づいてプリントジョブを暗号化することを可能とする。

【００５５】第２０の発明においては、第２の暗号化鍵情報記憶手段は前記暗号受信手段により前記所定の通信媒体を介して各画像処理装置から受信した複数の画像処理装置で共通する暗号化鍵情報を記憶して、いずれの画像処理装置に対しても対応する暗号化鍵情報に基づいて暗号化されたプリントジョブをグループ化されたいずれかの画像処理装置に転送可能とする。

【００５６】第２１の発明においては、前記暗号受信手段は、前記暗号化手段による暗号化開始直前に複数の画像処理装置で共通する暗号化鍵情報を受信して、複数の画像処理装置が通知する暗号化鍵情報が変更されても、常に復号可能となる最新の暗号化鍵情報に基づいてプリントジョブを暗号化することを可能とする。

【００５７】第２２の発明においては、プリントジョブは、画像処理装置における画像処理実行状態を制御するための所定の有効期限情報を含み、暗号化されたプリントジョブが画像処理装置側で復号化されても、有効期限外であれば当該プリントジョブの出力を制限することを可能とする。

【００５８】第２３の発明においては、暗号化手段は、画像処理装置における画像処理実行状態を制御するための所定の有効期限情報を含むプリントジョブを暗号化して、有効期限外であれば当該プリントジョブの出力を制限するための有効期限情報が容易に解読されてしまうことを防止することを可能とする。

【００５９】第２４の発明においては、前記プリントジョブ送信手段は、前記暗号化手段により暗号化されたプリントジョブおよび前記暗号化手段が暗号化に使用した前記所定の暗号化鍵情報も同時に画像処理装置に送信して、暗号化されたプリントジョブを受信する画像処理装置が当該暗号化鍵情報を識別することを可能とする。

【００６０】第２５の発明においては、前記プリントジョブ送信手段は、前記暗号化手段が暗号化に使用した前記所定の暗号化鍵情報をそのまま画像処理装置に送信して、暗号化されたプリントジョブを受信する画像処理装置が当該暗号化鍵情報が識別不能となる事態を回避することを可能とする。

【００６１】第２６の発明においては、通知手段による前記プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知すると、暗号受信手段がいずれかの画像処理装置から所定の暗号化鍵情報を受信し、該受信された前記所定の暗号化鍵情報に基づいて暗号化手段が作成されたプリントジョブを暗号化し、該暗号化されたプリントジョブをプリントジョブ送信手段が前記所定の暗号化鍵情報を受信した画像処理装置に送信し、プリントジョブ受信手段が前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信したら、復号手段が受信した暗号化されたプリントジョブを前記記憶手段に記憶された前記復号化鍵情報に基づいて復号化し、展開手段が該復号化したプリントジョブ中の各ページの画像データを画像メモリ上に展開して、いずれの情報処理装置に対しても同一の暗号化鍵情報で通知して暗号化されたプリントジョブの復号化処理を画一化し、かつ通信媒体上に出力された該プリントジョブは該暗号化鍵情報を提示した画像処理装置以外の画像処理装置では実質上復号化不能とした状態で転送し、該暗号化鍵情報を復号可能な画像処理装置の復号化鍵情報に基づいて画像出力可能なプリントジョブに復号してプリントジョブを処理することを可能とする。

【００６２】第２７の発明においては、いずれかの画像処理装置から所定の暗号化鍵情報を受信し、該受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化し、該暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置にプリントジョブ送信して、いずれの情報処理装置に対しても同一の暗号化鍵情報で通知して暗号化されたプリントジョブの復号化処理を画一化する処理を自動化することを可能とする。

【００６３】第２８の発明においては、プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知し、該通知された暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信し、該受信したプリントジョブを前記復号化鍵情報に基づいて復号化し、該復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開して、通信媒体上に出力された該プリントジョブは該暗号化鍵情報を提示した画像処理装置以外の画像処理装置では実質上復号化不能とした状態で転送し、該暗号化鍵情報を復号可能な画像処理装置の復号化鍵情報に基づいて画像出力可能なプリントジョブに復号する処理を自動化することを可能とする。

【００６４】

【実施例】

〔第１実施例〕図１は、本発明の第１の実施例を示す画像処理システムの構成を説明する概略ブロック図であり、該画像処理システムは、ネットワーク４を介して複数のコンピュータ２－１，２－２と、各画像形成装置１－１，１－２との画像処理を行う複数の画像処理装置３－１，３－２等から構成されている。

【００６５】なお、本実施例の場合、このネットワーク４はイーサネットで構成されているが、複数のコンピュータをネットワーク接続するものであれば、他のネットワークでも良い。このネットワークはローカルエリアネットワークであり、あるフロアやビル内のコンピュータを接続するのに使われる。

【００６６】図１において、画像処理装置３－１は、ネットワーク４を介して、自装置用の暗号化鍵ｆを、ネットワーク４上に接続されている各装置に送る。一方、別の画像処理装置３－２も、ネットワークを介して、自装置用の暗号化鍵ｇを、ネットワーク４上に接続されている各装置に送る。

【００６７】次に、コンピュータ２－１は、画像処理装置３－１と画像形成装置１－１を用いてプリントを行おうとする場合には、データ処理部２－１－１で作成したプリントするべきプリントジョブＴ１を、その内部の暗号化部２－１－２で、画像処理装置３－１用の暗号化鍵ｆ（該画像処理装置３－１から受信した暗号化鍵（暗号化鍵情報）ｆ）を用いて暗号化し、暗号化されたプリントジョブｆ（Ｔ１）をネットワーク経由で画像処理装置３－１に送出する。

【００６８】また、コンピュータ２－２が、画像処理装置３－１と画像形成装置１－１を用いてプリントを行おうとする場合にも同様に、データ処理部２－２－１で作

成したプリントするべきプリントジョブＴ２を、その内部の暗号化部２－２－２で、画像処理装置３－１用の暗号化鍵ｆ（該画像処理装置３－１から受信した暗号化鍵（暗号化鍵情報）ｆ）を用いて暗号化し、暗号化されたプリントジョブｆ（Ｔ２）をネットワーク経由で画像処理装置３－１に送出する。

【００６９】さらに、コンピュータ２－１は、画像処理装置３－２と画像形成装置１－２を用いてプリントを行おうとする場合には、プリントするべきプリントジョブＴ１を、その内部の暗号化部２－１－２で、画像処理装置３－２用の暗号化鍵ｇ（該画像処理装置３－２から受信した暗号化鍵（暗号化鍵情報）ｇ）を用いて暗号化し、暗号化されたプリントジョブｇ（Ｔ１）をネットワーク経由で画像処理装置３－２に送出する。

【００７０】また、コンピュータ２－２が、画像処理装置３－２と画像形成装置１－２を用いてプリントを行おうとする場合にも同様に、プリントするべきプリントジョブＴ２を、その内部の暗号化部２－２－２で、画像処理装置３－２用の暗号化鍵ｇ（該画像処理装置３－２から受信した暗号化鍵（暗号化鍵情報）ｇ）を用いて暗号化し、暗号化されたプリントジョブｇ（Ｔ２）をネットワーク経由で画像処理装置３－２に送出する。

【００７１】次に、暗号化鍵ｆを用いて暗号化されたプリントジョブｆ（Ｔ１）やプリントジョブｆ（Ｔ２）を受け取った画像処理装置３－１は、その内部の復号化部３－１－２で、暗号化鍵ｆに対応した復号鍵f^{-1}（後述するハードディスク８のプログラム領域８－２に記憶される）を用いて復号化して各プリントジョブＴ１やプリントジョブＴ２に戻し、画像処理部３－１－１により各プリントジョブＴ１，Ｔ２に含まれるＰＤＬデータをＲＡＭ１０のフルページ画像メモリ１０－１にラスタ画像として展開して画像形成装置１－１に送り、画像形成を行う。

【００７２】また、暗号化鍵ｇを用いて暗号化されたプリントジョブｇ（Ｔ１）やプリントジョブｇ（Ｔ２）を受け取った画像処理装置３－２も、その内部の復号化部３－２－２で、暗号化鍵ｇに対応した復号鍵g^{-1}を用いて復号化して各プリントジョブＴ１やプリントジョブＴ２に戻し、画像処理部３－２－１により各プリントジョブＴ１，Ｔ２に含まれるＰＤＬデータをＲＡＭ１０のフルページ画像メモリ１０－１にラスタ画像として展開して画像形成装置１－２に送り、画像形成を行う。

【００７３】本実施例で用いる暗号化鍵、復号化鍵は、ＲＳＡ暗号に代表される、公開鍵暗号方式の暗号化鍵、復号化鍵を用いている。この方式では、暗号化鍵から復号化鍵を求めるのが実質上不可能という性質があるため、暗号化鍵を公開できるという特徴がある。

【００７４】一般に、プリンタ（画像形成装置１－１，１－２）は不特定多数の複数のホストコンピュータからのプリントジョブを受け付けなくてはならないという環境的特徴があるため、１対１の暗号化手法は適していないし、暗号化鍵を秘密にすべき暗号化手法は適していない。これに対し、公開鍵暗号方式を用いると、各画像処理装置固有の単一の暗号化鍵を全てのホストコンピュータに公開でき、その暗号化鍵で暗号化したプリントジョブは、その暗号化鍵に対応する画像処理装置以外では復号化できないという点でプリンタに適している。

【００７５】図２は、図１に示した画像処理装置３－１，３－２と画像形成装置１－１，１－２とから構成される画像処理システムの要部構成を説明するブロック図である。

【００７６】この図に示すように、ホストコンピュータ２－１，２－２等と、画像処理装置３－１（以下、画像処理装置３－１を例とする）とはネットワーク４を介して接続されている。ホストコンピュータ（コンピュータ２－１～２－３のいずれかのコンピュータ）からネットワーク４および外部インタフェース５を介して送られてきたＰＤＬデータは、ＣＰＵ６によって一旦、ハードディスク８内のスプール用領域８－１内に保持される。

【００７７】次いで、スプール用領域８－１から読み出されたＰＤＬデータはラスタイメージ画像データに展開され、ＲＡＭ１０内のフルページ画像メモリ１０－１に書き込まれ、該展開された画像データは、フルページ画像メモリ１０－１から読み出され、プリンタインタフェース１１を経由して画像形成装置１に送られ画像が形成される。

【００７８】ハードディスク８内のプログラム領域８－２はプログラムを保持するのに使われ、それがＲＡＭ１０内のワークメモリ領域１０－２に移されてプログラムが実行される。ワークメモリ領域１０－２の一部や、ハードディスク８内のワークメモリ領域８－３は作業用の一時領域としても使われる。プリンタ通信部９は画像形成装置１との通信を行うためのものである。

【００７９】また、７は各デバイス間とを結ぶＣＰＵバスである。本実施例においては、暗号化鍵、復号化鍵はプログラム領域８－２内に、別の暗号化処理を施された形で保持されていて、書き換えられることはない。

【００８０】フルページ画像メモリ１０－１は本実施例では、１画素につきＲＧＢ（Red,Green,Blue）各８ｂｉｔ、計２４ｂｉｔで構成され、Ａ３サイズ１ページ分の容量を持ち、Ａ４サイズをプリントする場合は２ページ分の容量となる。

【００８１】本実施例における画像形成装置１－１は、フルカラーの電子写真複写機であり、画像処理装置から送られる１画素につきＲＧＢ各８ｂｉｔ、計２４ｂｉｔのラスタ形式の画像データ１２に基づいて画像形成を行う。ただし、画像形成はＹＭＣＫ（Yellow,Magenta,Cyan,Black）の４色のトナーを用いて行われるため、画像形成装置１内部でＲＧＢからＹＭＣＫへの変換が行われる。

【００８２】次に、ＰＤＬデータについて説明する。

【００８３】アドビ（ＡＤＯＢＥ）社のＰｏｓｔＳｃｒｉｐｔ（登録商標）言語に代表されるＰＤＬ（Page Description Language）は、１ページの画像を、（ｉ）文字コードによる画像記述、（ｉｉ）図形コードによる画像記述、（ｉｉｉ）ラスタ画像データによる画像記述などの要素を組み合わせて記述するための言語であり、それで記述されたデータがＰＤＬデータである。

【００８４】該ＰＤＬデータはこのように文字コードや図形コード、言い換えると図形描画コマンドを中心として構成されているので、ラスタ画像データのみの場合に比べて、一般にプリントジョブのデータ量が少なくて済む。このため、暗号化処理や復号化処理を行う場合に、処理時間が少なくて済むという利点がある。

【００８５】また、ＰＤＬデータには可読性を向上するため、人間が読むことのできるアスキーデータで構成されている場合がある。この場合は、暗号化処理を行わないと、プリントジョブの中身を見られる危険性がさらに大きくなるという特徴を持っている。一方、プリントジョブがラスタ画像データのみの場合は、人間が読むことができないので比較的安全である。

【００８６】図３は、図１に示したコンピュータと画像処理装置との間におけるプリントジョブの暗号化／複合化処理状態を説明する模式図であり、コンピュータ上で生成されたプリントジョブが、暗号化され、ネットワーク４を経由して画像処理装置に送られ、復号化されて元のプリントジョブに戻るまでの状態に対応する。

【００８７】本実施例の画像処理装置は、暗号化鍵と復号化鍵の組み合わせを２種類保持している。１つは１台の画像処理装置３に固有の個別鍵であり、もう１つは、複数台の画像処理装置３で共有するグループ別鍵である。個別暗号化鍵で暗号化したジョブは、個別復号化鍵を持った１台の画像処理装置でないと復号化できない。

【００８８】一方、グループ別暗号化鍵で暗号化したジョブは、グループ別復号化鍵を持った複数台の画像処理装置のうちのどれかであれば復号化できる。また、本実施例の画像処理装置は、２種類の暗号化鍵で暗号化されたジョブの他に、暗号化されていないジョブも受け取れる構成になっている。

【００８９】図３において、暗号化しない場合は、コンピュータ上で生成されたプリントジョブＴ１は、そのまま、ネットワーク４を経由して画像処理装置に送られる。この場合、プリントジョブの一部に暗号化されていないことを示す情報として、「０」が付加される。

【００９０】次に、個別暗号化鍵ｆで暗号化する場合は、プリントジョブＴ１は、コンピュータで暗号化されてプリントジョブｆ（Ｔ１）となり、その状態でネットワーク４を経由して画像処理装置に送られ、個別暗号化鍵ｆに対応する個別復号化鍵f^{-1}を用いて復号化される。この場合、プリントジョブの一部に個別暗号化鍵ｆで暗号化したことを示す情報として、暗号化鍵ｆが暗号化されない状態で付加される。

【００９１】次に、グループ別暗号化鍵ｈで暗号化する場合は、プリントジョブＴ１は、暗号化されてプリントジョブｈ（Ｔ１）となり、その状態でネットワーク４を経由して画像処理装置に送られ、グループ別暗号化鍵ｈに対応するグループ別復号化鍵h^{-1}を用いて復号化される。

【００９２】この場合、プリントジョブの一部にグループ別暗号化鍵ｈで暗号化したことを示す情報として、暗号化鍵ｈが暗号化されない状態で付加される。

【００９３】図３において、プリントジョブに暗号化鍵を付加しているのは、プリントジョブを受け取った画像処理装置が、そのプリントジョブが、暗号化されていないか、または、その装置の個別暗号化鍵を用いて暗号化されているか、または、その装置のグループ別暗号化鍵を用いて暗号化されているかを、または、他装置の個別／グループ別暗号化鍵を用いて暗号化されているかを、復号化を試みることなく簡単に判断するためである。

【００９４】このため、暗号化鍵は暗号化されない状態で付加される。また、本実施例では、暗号化状態を識別するための情報として暗号化鍵そのものを用いたが、その代わりに別の識別番号等を使ってもよい。

【００９５】また、暗号化していないことを示す情報として「０」という暗号化鍵を付加するようにしたが、暗号化していないことを示すものであれば何でもよい。

【００９６】図４は、図２に示したハードディスク８のスプール領域に配置される待ち行列を説明するための図である。

【００９７】この図に示すように、第１実施例の画像処理装置は、ホストコンピュータから受け取ったジョブをハードディスク８内のスプール領域８－１に保持するが、その保持場所として３種類の待ち行列を使用している。

【００９８】図４に示すごとく、１つ目はプリントキューＰＣと呼ばれる待ち行列で、この待ち行列は待ち行列に入った順番にジョブが並び、先頭のジョブからプリントが実行される仕組みになっている。

【００９９】２つ目はホールドキューＨＣと呼ばれる待ち行列で、この待ち行列でも待ち行列に入った順番にジョブが並ぶが、ホールドキューＨＣ中のジョブはユーザにより意図的にプリントキューＰＣに移動されない限りプリントされない。

【０１００】なお、プリントキューＰＣに移動する場合は、図４に示すごとく、プリントキューＰＣの最後に移動される。

【０１０１】３つ目は完了キューＥＣと呼ばれる待ち行列で、この待ち行列でも待ち行列に入った順番にジョブが並ぶが、完了キューＥＣ中のジョブもユーザにより意図的にプリントキューＰＣに移動されない限りプリント

されない。また、プリントキューＰＣ、ホールドキューＨＣは、ホストコンピュータから受け取ったジョブを保持しておくためのキューであり、一方、完了キューＥＣはプリントの終了したジョブを自動的に保持しておくためのキューである。

【０１０２】プリントの終了したジョブは、図４に示すごとく、完了キューＥＣの最後に移動される。完了キューＥＣ中のジョブは完了キューＥＣに入って一定時間後に消される仕組みになっている。プリントキューＰＣ、ホールドキューＨＣ、完了キューＥＣ中のジョブは不図示の操作部によりキュー間で移動できる構成となっている。

【０１０３】本実施例の画像処理装置では、ホストコンピュータから画像処理装置３－１にプリントジョブを送る場合、プリントキューＰＣとホールドキューＨＣのどちらのキューに入れるかを指定する仕組みになっている。

【０１０４】本実施例では、各キューにおけるジョブは、それをホストコンピュータから受け取ったままの状態で保持される。即ち、暗号化されなかったジョブは暗号化されない状態のまま、暗号化されたジョブは暗号化された状態のまま、各キューに保持される。暗号化されたジョブは、プリントキューＰＣの先頭に到達した場合に初めて、復号化され、展開されてプリントされる。

【０１０５】そして、プリント後は、復号化された方のジョブではなく、復号化される前のジョブの方が完了キューＥＣに移される。以上の処理は、展開中以外に復号化した状態を持たないことにより、復号化した状態のプリントジョブを盗まれたり、中身を見られたりする危険性をなくすことを可能としている。

【０１０６】また、ホストコンピュータからプリントジョブに付加されて受け取った暗号化鍵は、そのまま、付加された状態で各キューに保持される。

【０１０７】以下、本実施例と第１～第７，第９～第１８，第２０～第２６の発明の各手段との対応およびその作用について図１～図４等を参照して説明する。

【０１０８】第１の発明は、所定の通信媒体（ネットワーク４）を介して複数の情報処理装置（コンピュータ２－１，２－２）から受信したプリントジョブに基づいて画像処理を行う画像処理装置３－１，３－２において、前記プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知する通知手段（外部インタフェース５）と、前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信するプリントジョブ受信手段（外部インタフェース５）と、前記暗号化鍵情報に対応した復号化鍵情報を記憶する記憶手段（ワークメモリ領域８－３）と、受信したプリントジョブを前記復号化鍵情報に基づいて復号化する復号手段（プログラム領域８－２に記憶された復号処理プログラムをＣＰＵ６が実行して復号する）と、画像データを記憶する画像メモリ手段（フルページ画像メモリ１０－１）と、復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開する展開手段（プログラム領域８－２に記憶された展開処理プログラムをＣＰＵ６が実行して展開する）とを設け、外部インタフェース５による前記プリントジョブを暗号化するための暗号化鍵情報を各コンピュータ２－１，２－２に通知後、外部インタフェース５が前記暗号化鍵情報により暗号化されたプリントジョブを各コンピュータ２－１，２－２から受信したら、ＣＰＵ６が受信した暗号化されたプリントジョブをワークメモリ領域８－３に記憶された前記復号化鍵情報に基づいて復号化し、ＣＰＵ６が該復号化したプリントジョブ中の各ページの画像データをフルページ画像メモリ１０－１上に展開して、通信媒体上に出力された該プリントジョブは該暗号化鍵情報を提示した画像処理装置以外の画像処理装置では実質上復号化不能とした状態で転送し、該暗号化鍵情報を復号可能な画像処理装置の復号化鍵情報に基づいて画像出力可能なプリントジョブに復号してプリントジョブを処理することを可能とする。

【０１０９】第２の発明は、前記通知手段（外部インタフェース５）は、同一の暗号化鍵情報を前記通信媒体（ネットワーク４）を介して各情報処理装置（ホストコンピュータ２－１，２－２）に通知して、プリントジョブを暗号化するための暗号化鍵情報を全ての情報処理装置に対して共通化することを可能とする。

【０１１０】第３の発明は、所定のネットワーク４を介して暗号化鍵情報を複数の情報処理装置に通知して、各情報処理装置（ホストコンピュータ２－１，２－２）に通知した暗号化鍵情報を容易に変更可能とする。

【０１１１】第４の発明は、復号手段（ＣＰＵ６による）は、画像データの展開の直前、もしくは展開中に前記受信した暗号化されたプリントジョブの復号を行い、暗号化されたプリントジョブ全体が復号化されてしまう事態を回避することを可能とする。

【０１１２】第５の発明は、暗号化鍵情報に対する前記復号化鍵情報との組合せを複数備え、他の画像処理装置と共有してあるいは各画像処理装置固有にプリントジョブを暗号化／復号化する異なる環境を共存させることを可能とする。

【０１１３】第６の発明は、前記プリントジョブに付加された有効期限情報（例えば時間単位）に基づいて受信したプリントジョブの処理を制御する第１の制御手段（ＣＰＵ６による）を有し、ＣＰＵ６は前記プリントジョブに付加された有効期限情報に基づいて受信したプリントジョブの処理を制御して、暗号化されたプリントジョブが転送中に第３者により入手されてしまっても、有効期限情報の制約に合致しない場合には、復号化できたプリントジョブであってもその画像出力を確実に制限することを可能とする。

【０１１４】第７の発明は、有効期限情報は、暗号化された状態で前記プリントジョブに付加して、有効期限情報の書き換えを防止することを可能とする。

【０１１５】第９の発明は、プリントジョブ受信手段（外部インタフェース５）は、前記暗号化鍵情報により暗号化されたプリントジョブおよび暗号化鍵情報を併せて各情報処理装置から受信して、受信したプリントジョブの暗号化状態を確実に識別して、対応する最適な復号化鍵情報に基づいて受信したプリントジョブを正常に復号化することを可能とする。

【０１１６】第１０の発明は、プリントジョブ受信手段（外部インタフェース５）が各情報処理装置（ホストコンピュータ２－１，２－２）から受信する暗号化鍵情報は暗号化されていない状態で受信し、受信した暗号化鍵情報と通知した暗号化鍵情報とから暗号化に使用された暗号化鍵情報を確実に識別することを可能とする。

【０１１７】第１１の発明は、前記暗号化鍵情報により暗号化されたプリントジョブを印刷候補として複数一時的に保持する第１の保持手段（スプール用領域８－１のプリントＰＣ）を有し、プリントＰＣが前記暗号化鍵情報により暗号化されたプリントジョブを印刷候補として複数一時的に保持して、印刷候補となるプリントジョブ自体は印刷される直前まで暗号化された状態で保持することを可能とする。

【０１１８】第１２の発明は、前記暗号化鍵情報により暗号化されたプリントジョブを出力待機候補として複数一時的にそのまま保持第２の保持する手段（スプール用領域８－１のホールドキューＨＣ）を有し、ホールドキューＨＣが前記暗号化鍵情報により暗号化されたプリントジョブを出力待機候補として複数一時的にそのまま保持して、出力待機状態となっているプリントジョブ自体は印刷される直前まで暗号化された状態で保持することを可能とする。

【０１１９】第１３の発明は、前記展開手段により画像メモリ上に展開された画像データを画像出力装置（画像形成装置１－１，１－２）に送出する送出手段（画像処理部３－１－１，３－２－１）と、前記送出手段により前記画像出力装置に送出されて画像出力が完了した前記暗号化鍵情報により暗号化されたプリントジョブを破棄候補として複数一時的に保持する第３の保持手段（スプール用領域８－１の完了キューＥＣ）を有し、ＣＰＵ６によりフルページ画像メモリ１０－１上に展開された画像データが画像処理部３－１－１，３－２－１により画像形成装置１－１，１－２に送出されて、前記画像出力装置による画像出力が完了したら、完了キューＥＣが前記暗号化鍵情報により暗号化されたプリントジョブを破棄候補として複数一時的に保持して、復号化されて画像出力装置から出力されてしまったプリントジョブがそのままの状態で保持されてしまうことを回避することを可能とする。

【０１２０】第１４の発明は、前記展開手段（ＣＰＵ６による）によりフルページ画像メモリ１０－１上に展開された画像データを画像出力装置（画像形成装置１－１，１－２）に送出する送出手段（画像処理部３－１－１，３－２－１）と、前記送出手段により前記画像出力装置に送出されて画像出力が完了した前記暗号化鍵情報により暗号化されていないプリントジョブを破棄候補として複数一時的に保持する第３の保持手段（スプール用領域８－１の完了キューＥＣ）を有し、ＣＰＵ６により画像メモリ上に展開された画像データが画像処理部３－１－１，３－２－１により画像形成装置１－１，１－２に送出されて、画像形成装置１－１，１－２による画像出力が完了したら、完了キューＥＣが前記暗号化鍵情報により暗号化されていないプリントジョブを破棄候補として複数一時的に保持して、画像出力が完了している暗号化されていたプリントジョブが不用意に保持される状態を回避することを可能とする。

【０１２１】第１５の発明は、前記暗号化されたプリントジョブは、所定のページ記述言語（ポストスクリプト，ＬＩＰＳＩＩＩ，ＣａＰＳＬ等（商品名を含む））で記述された印刷情報を暗号化鍵情報に基づいて暗号化して、ページ記述言語中で容易に可読できるデータを確実に暗号化して転送して処理することを可能とする。

【０１２２】第１６の発明は、前記暗号化鍵情報と対となる復号化鍵情報は、所定の公開鍵暗号方式に準拠し、プリントジョブの暗号化／復号化処理環境を容易に構築することを可能とする。

【０１２３】第１７の発明は、所定の通信媒体を介して複数の画像処理装置と通信可能な情報処理装置（コンピュータ２－１，２－２）において、いずれかの画像処理装置から所定の暗号化鍵情報を受信する暗号受信手段（データ処理部２－１－１，２－２－１のインタフェース部）と、前記暗号受信手段により受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化する暗号化手段（暗号化部２－１－２，２－２－２）と、前記暗号化手段により暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置に送信するプリントジョブ送信手段（データ処理部２－１－１，２－２－１のインタフェース部）とを有し、データ処理部２－１－１，２－２－１のインタフェース部がいずれかの画像処理装置から所定の暗号化鍵情報を受信したら、該受信された前記所定の暗号化鍵情報に基づいて暗号化部２－１－２，２－２－２が作成されたプリントジョブを暗号化し、該暗号化されたプリントジョブを上記インタフェース部が前記所定の暗号化鍵情報を受信した画像処理装置３－１，３－２に送信して、いずれの情報処理装置に対しても同一の暗号化鍵情報で通知して暗号化されたプリントジョブの復号化処理を画一化することを可能とする。

【０１２４】第１８の発明は、データ処理部２－１－

１，２－２－１のインタフェース部により前記所定の通信媒体（ネットワーク４）を介して各画像処理装置３－１，３－２から受信した固有の暗号化鍵情報を記憶する第１の暗号化鍵情報記憶手段（図示しないＲＡＭ，ハードディスク）を設け、第１の暗号化鍵情報記憶手段が前記暗号受信手段により前記所定の通信媒体を介して各画像処理装置から受信した固有の暗号化鍵情報（ｆ）を記憶して、いずれの画像処理装置に対しても対応する暗号化鍵情報に基づいて暗号化されたプリントジョブを転送可能とする。

【０１２５】第２０の発明は、データ処理部２－１－１，２－２－１のインタフェース部により前記所定の通信媒体を介して各画像処理装置から受信した複数の画像処理装置３－１，３－２で共通する暗号化鍵情報を記憶する第２の暗号化鍵情報記憶手段（図示しないＲＡＭ，ハードディスク）を設け、第２の暗号化鍵情報記憶手段は前記暗号受信手段により前記所定の通信媒体を介して各画像処理装置から受信した複数の画像処理装置３－１，３－２で共通する暗号化鍵情報（ｇ）を記憶して、いずれの画像処理装置に対しても対応する暗号化鍵情報に基づいて暗号化されたプリントジョブをグループ化されたいずれかの画像処理装置に転送可能とする。

【０１２６】第２１の発明は、前記暗号受信手段（データ処理部２－１－１，２－２－１のインタフェース部）は、前記暗号化部２－１－２，２－２－２による暗号化開始直前に複数の画像処理装置で共通する暗号化鍵情報を受信して、複数の画像処理装置が通知する暗号化鍵情報が変更されても、常に復号可能となる最新の暗号化鍵情報に基づいてプリントジョブを暗号化することを可能とする。

【０１２７】第２２の発明は、プリントジョブは、画像処理装置における画像処理実行状態を制御するための所定の有効期限情報を含み、暗号化されたプリントジョブが画像処理装置側で復号化されても、有効期限外であれば当該プリントジョブの出力を制限することを可能とする。

【０１２８】第２３の発明は、暗号化手段（暗号化部２－１－２，２－２－２）は、画像処理装置３－１，３－２における画像処理実行状態を制御するための所定の有効期限情報を含むプリントジョブを暗号化して、有効期限外であれば当該プリントジョブの出力を制限するための有効期限情報が容易に解読されてしまうことを防止することを可能とする。

【０１２９】第２４の発明は、前記プリントジョブ送信手段（データ処理部２－１－１，２－２－１のインタフェース部）は、前記暗号化手段（暗号化部２－１－２，２－２－２）により暗号化されたプリントジョブおよび前記暗号化手段が暗号化に使用した前記所定の暗号化鍵情報も同時に画像処理装置に送信して、暗号化されたプリントジョブを受信する画像処理装置が当該暗号化鍵情報を識別することを可能とする。

【０１３０】第２５の発明は、前記プリントジョブ送信手段（データ処理部２－１－１，２－２－１のインタフェース部）は、前記暗号化手段（暗号化部２－１－２，２－２－２）が暗号化に使用した前記所定の暗号化鍵情報をそのまま画像処理装置３－１，３－２に送信して、暗号化されたプリントジョブを受信する画像処理装置が当該暗号化鍵情報が識別不能となる事態を回避することを可能とする。

【０１３１】第２６の発明は、所定の通信媒体（ネットワーク４）を介して複数の画像処理装置３－１，３－２と複数の情報処理装置（コンピュータ２－１，２－２）とが通信可能な画像処理システムにおいて、いずれかの画像処理装置から所定の暗号化鍵情報を受信する暗号受信手段（データ処理部２－１－１，２－２－１のインタフェース部）と、前記暗号受信手段により受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化する暗号化手段（暗号化部２－１－２，２－２－２）と、前記暗号化手段により暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置に送信するプリントジョブ送信手段（データ処理部２－１－１，２－２－１のインタフェース部）とを有する情報処理装置と、所定の通信媒体を介して複数の情報処理装置から受信したプリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知する通知手段（外部インタフェース５）、前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信するプリントジョブ受信手段（外部インタフェース５）、前記暗号化鍵情報に対応した復号化鍵情報を記憶する記憶手段（ワークメモリ領域８－３）と、受信したプリントジョブを前記復号化鍵情報に基づいて復号化する復号手段（プログラム領域８－２に記憶された復号処理プログラムをＣＰＵ６が実行して復号する）、画像データを記憶する画像メモリ手段（フルページ画像メモリ１０－１）と、復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開する展開手段（プログラム領域８－２に記憶された展開処理プログラムをＣＰＵ６が実行して展開する）とを有し、外部インタフェース５による前記プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置（コンピュータ２－１，２－２）に通知すると、データ処理部２－１－１，２－２－１のインタフェース部がいずれかの画像処理装置から所定の暗号化鍵情報を受信し、該受信された前記所定の暗号化鍵情報に基づいて暗号化部２－１－２，２－２－２が作成されたプリントジョブを暗号化し、該暗号化されたプリントジョブを上記インタフェース部が前記所定の暗号化鍵情報を受信したコンピュータ２－１，２－２に送信し、外部インタフェース５が前記暗号化鍵情報により暗号化されたプリントジョブを各コンピュータ２－１，２－２から受信したら、ＣＰＵ

６が受信した暗号化されたプリントジョブをワークメモリ領域８－３に記憶された前記復号化鍵情報に基づいて復号化し、ＣＰＵ６が該復号化したプリントジョブ中の各ページの画像データをフルページ画像メモリ１０－１上に展開して、いずれの情報処理装置に対しても同一の暗号化鍵情報で通知して暗号化されたプリントジョブの復号化処理を画一化し、かつ通信媒体上に出力された該プリントジョブは該暗号化鍵情報を提示した画像処理装置以外の画像処理装置では実質上復号化不能とした状態で転送し、該暗号化鍵情報を復号可能な画像処理装置の復号化鍵情報に基づいて画像出力可能なプリントジョブに復号してプリントジョブを処理することを可能とする。

【０１３２】〔第１データ処理方法〕図５は、本発明に係る画像処理システムのデータ処理方法の第１実施例を示すフローチャートであり、外部装置であるホストコンピュータ２－１側のプリント時の制御手順に対応する。なお、（１）～（７）は各ステップを示す。

【０１３３】まず、ステップ（１）でプリントすべきプリンタを選択する。これは、ネットワーク４に接続されているプリンタの一覧を表示して選択したり、あらかじめ登録してあるプリンタの中から選んだりする。この場合のプリンタとは画像処理装置３－１と画像形成装置１－１とのペアを意味する。

【０１３４】次に、ステップ（２）で、選択されたプリンタに対し、ネットワーク経由で暗号化鍵の問い合わせを行う。この場合、通常は個別暗号化鍵を要求するが、グループ別暗号化鍵を要求してもよい。この問い合わせに対し、ネットワーク経由で暗号化鍵が画像処理装置３－１から送られてくるので、それをデータ処理部２－１－１のワークメモリに保持する。

【０１３５】次に、ステップ（３）でプリンタの変更を操作者が指定しているかどうかを判定し、指定していればステップ（１）に戻って再度プリントの選択から繰り返す。

【０１３６】一方、ステップ（３）でプリンタの変更を指定していないと判定した場合には、ステップ（４）でプリント要求があるかどうか判定し、ないと判定された場合はステップ（３）に戻り、プリント要求があると判定された場合は、ステップ（５）で暗号化が必要かどうかを操作者の指定、文書のセキュリティレベル等から判断し、暗号化が必要でないと判定された場合は、ステップ（７）に進み、暗号化が必要であると判定された場合は、ステップ（６）において、まずそのジョブの有効期限情報を付加し、ステップ（２）で受け取った暗号化鍵を用いて有効期限情報を含んだ形で暗号化する。

【０１３７】なお、本実施例において、有効期限情報とは、このジョブをプリンタに送信後、プリンタにおいて指定した有効期限以内であればプリントし、有効期限以後はプリントしないことを指定するための情報であり、有効期限としては、各プリントシステムのニーズにより違うが、例えば１時間等でよい。この有効期限は、プリントジョブがネットワーク転送中に盗まれ、後日、プリントされることを防止することが可能となる。

【０１３８】また、有効期限情報を暗号化するのは、有効期限情報を書き換えられないようにするためである。

【０１３９】そして、ステップ（７）では必要に応じて暗号化処理されたプリントジョブを暗号化に使用した暗号化鍵と共に、ステップ（１）で選択されたプリンタに送付する。ただし、暗号化を行わなかった場合は、暗号化鍵として「０」を送付する。また、暗号化鍵自体は暗号化せずに送付するのは上述の通りである。

【０１４０】なお、ステップ（７）でのプリントジョブの送出時に、選択したプリンタが電源オフだった場合や、紙なし等によりプリントジョブを受けられない場合は、図５には記述していないが、ステップ（１）に戻りプリンタ選択から再度、全ての処理をやり直す。

【０１４１】ただし、１回目のプリンタ選択時にステップ（２）でグループ別暗号化鍵を問い合わせ、それを用いて暗号化処理を行った場合は、２回目のプリンタ選択時に同じグループに属するプリンタを選択することにより、ステップ（２）～（６）の処理を再度行うことなく、ステップ（７）で暗号化されたプリントジョブをプリンタに送付できる。

【０１４２】なお、グループ別暗号化鍵はこのような場合以外にも、プリンタからプリンタへのジョブの転送を可能にしたり、また、各プリンタの暗号化鍵を全て保持する場合のメモリ量の削減に効果がある。

【０１４３】図６は、本発明に係る画像処理システムのデータ処理方法の第１実施例を示すフローチャートであり、画像処理装置３の受信タスク処理に対応する。なお、（１）～（６）は各ステップを示す。

【０１４４】まず、ステップ（１）でホストコンピュータから暗号化鍵の送付要求があるかどうか判定し、あると判定した場合には、ステップ（２）で暗号化鍵をネットワーク経由で送付する。通常は、個別暗号化鍵を送付するが、送付要求の内容に応じてグループ別暗号化鍵を送付する。送付後はステップ（１）に戻る。

【０１４５】一方、ステップ（１）で送付要求が無いと判定した場合は、ステップ（３）でジョブの受信要求があるかどうか判定し、ないと判定した場合には、ステップ（１）に戻る。

【０１４６】一方、ステップ（３）で受信要求があると判定した場合は、ステップ（４）で受信要求のあったジョブの行き先指定がホールドキューかどうか判定し、ホールドキューであると判定した場合は、ステップ（５）で、受信したジョブをホールドキューの最後に追加しステップ（１）に戻る。

【０１４７】一方、ステップ（４）で、ホールドキューでないと判定された場合は、ステップ（６）で、受信し

たジョブをプリントキューの最後に追加する。

【０１４８】図７は、図２に示した画像処理装置による第１のプリントタスクの一例を示すフローチャートである。なお、（１）～（１１）は各ステップを示す。

【０１４９】まず、ステップ（１）でプリントキューの先頭のジョブをピックアップする。ステップ（２）ではピックアップしたジョブが、暗号化されていないか、暗号化されている場合は、どの暗号化鍵で暗号化されているかを、ジョブに付加された暗号化鍵で判断（暗号化鍵自体は暗号化されていないので直ちに判断できる）し、ジョブに付加された暗号化鍵が暗号化していないことを意味する「０」の場合は、ステップ（１０）で、そのジョブの各ページを順次、フルページ画像メモリ１０－１上に展開し、ステップ（１１）で展開した画像データを画像形成装置１－１に送ってプリントを行い、全てのページをプリント後、ステップ（９）でプリント終了したジョブを完了キューＥＣに移動し、ステップ（１）に戻る。

【０１５０】一方、ステップ（２）で、自装置の個別暗号化鍵とジョブに付加された暗号化鍵が一致した場合は、ステップ（３）で自装置の個別暗号化鍵に対応した個別復号化鍵を準備し、ステップ（５）に移る。

【０１５１】一方、ステップ（２）で自装置のグループ別暗号化鍵とジョブに付加された暗号化鍵が一致した場合は、ステップ（４）で自装置のグループ別暗号化鍵に対応したグループ別復号化鍵を準備し、ステップ（５）に移る。

【０１５２】一方、ステップ（２）で自装置の個別暗号化鍵とも、グループ別暗号化鍵とも、ジョブに付加された暗号化鍵が一致しない場合は、図７には記述していないが、そのジョブを削除してステップ（１）に戻る。

【０１５３】次に、ステップ（５）では、ステップ（３）、またはステップ（４）で準備された復号化鍵を用いて復号化しつつ、そのジョブの各ページを順次、フルページ画像メモリ１０－１上に展開する。

【０１５４】なお、本実施例では復号化と展開を同時に行うことにより、全体が復号化されたプリントジョブを作らないようにしている。

【０１５５】次に、ステップ（６）では、復号化されたジョブ内に含まれる有効期限情報をチェックし、ワークメモリ領域１０－２に保持される有効期限内かどうか判定し、有効期限が切れていたらステップ（７）でジョブを削減し、画像メモリ内の情報をクリアしてステップ（１）に戻る。

【０１５６】一方、有効期限内であれば、ステップ（８）で、展開した画像データを画像形成装置１に送ってプリントを行う。

【０１５７】なお、図７には記載していないが、ステップ（５）からステップ（８）までの処理を、そのジョブの各ページについて順次行う。全てのページをプリント後、ステップ（９）でプリント終了したジョブを完了キューＥＣに移動し、画像メモリ内の情報をクリアしてステップ（１）に戻る。

【０１５８】このとき、暗号化されたジョブについてはステップ（５）で復号化した状態ではなく、復号する前の状態のものをプリントキューＰＣから移動する。

【０１５９】以下、本実施例と第２７，第２８の発明の各工程との対応およびその作用について図５～図７等を参照して説明する。

【０１６０】第２７の発明は、所定の通信媒体（ネットワーク４）を介して複数の画像処理装置（３－１，３－２）と複数の情報処理装置とが通信可能な画像処理システムのジョブ処理方法において、いずれかの画像処理装置から所定の暗号化鍵情報を受信する暗号受信工程（図５のステップ（２））と、該受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化する暗号化工程（図５のステップ（５））と、該暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置にプリントジョブ送信する送信工程（図５のステップ（７））とを実行して、いずれの情報処理装置に対しても同一の暗号化鍵情報で通知して暗号化されたプリントジョブの復号化処理を画一化する処理を自動化することを可能とする。

【０１６１】第２８の発明は、所定の通信媒体（ネットワーク４）を介して複数の画像処理装置（３－１，３－２）と複数の情報処理装置とが通信可能な画像処理システムのジョブ処理方法において、プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知する通知工程（図６のステップ（１），（２））、前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信するプリントジョブ受信工程（図６のステップ（３）～（６））、受信したプリントジョブを前記復号化鍵情報に基づいて復号化する復号工程（図７のステップ（１）～（５））と、該復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開する展開工程（図７のステップ（５））とを実行して、通信媒体上に出力された該プリントジョブは該暗号化鍵情報を提示した画像処理装置以外の画像処理装置では実質上復号化不能とした状態で転送し、該暗号化鍵情報を復号可能な画像処理装置の復号化鍵情報に基づいて画像出力可能なプリントジョブに復号する処理を自動化することを可能とする。

【０１６２】上記第１実施例では、復号化と展開を同時に行うことにより、全体が復号化されたプリントジョブを作らないようにしているが、暗号化されたプリントジョブ全体を復号化して一時メモリに入れた後、展開し、展開後は一時メモリ内の復号化されたジョブを消去するようにしてもよい。

【０１６３】また、第１実施例では、暗号化に使用した暗号化鍵を付加して、これで暗号化の種類や、暗号化さ

れているかいないかを判断したが、これをとにかく自装置の復号化鍵で復号化してみて、意味のあるデータにあるかどうかで判断したり、また、意味があるかどうかに関わらず、復号化したデータをそのまま処理するようにしてもよい。

【０１６４】後者の場合は、正しく復号化されない場合は、その処理においてエラーとなり、エラー処理される。

【０１６５】〔第２実施例〕第１実施例では暗号化鍵が固定である場合について説明したが、暗号化鍵を可変とし、また、暗号化鍵を送付するタイミング、ジョブを作成したコンピュータとジョブを送付したコンピュータが同一かどうかを確認し、さらに、暗号化ジョブをホールドキューＨＣ、完了キューＥＣに入れないように制御する構成としてもよい。以下、その実施例と第８，第１９の発明の各手段との対応およびその作用について図１～図４等を参照して説明する。なお、第１実施例と同様のハードな部分については説明を省略し、第１実施例と異なる部分についてのみ、図８、図９、図１０を用いて説明する。

【０１６６】第８の発明は、受信したプリントジョブを作成した情報処理装置と受信したプリントジョブを送信した情報処理装置とが同一であるか認証する認証手段（ＣＰＵ６がプログラム領域８－２に記憶された認証処理プログラムに基づいて認証する）と、前記認証手段の認証結果に基づいて受信したプリントジョブの処理を制御する第２の制御手段（ＣＰＵ６による）とを有し、ＣＰＵ６により受信したプリントジョブを作成した情報処理装置と受信したプリントジョブを送信した情報処理装置とが同一であるかを認証し、該認証結果に基づいて受信したプリントジョブの処理を制御して、いずれかの情報処理装置が通知された暗号化鍵情報に基づいて暗号化されたプリントジョブを他の情報処理装置が取得する事態が発生しても、該他の情報処理装置から取得したプリントジョブを対応する画像処理装置から出力されてしまう事態を確実に制限することを可能とする。

【０１６７】第１９の発明は、暗号受信手段（コンピュータ２－１，２－２のインタフェース部）は、前記暗号化部２－１－２，２－２－２による暗号化開始直前に各画像処理装置から前記固有の暗号化鍵情報を受信して、各画像処理装置が通知する暗号化鍵情報が変更されても、常に復号可能となる最新の暗号化鍵情報に基づいてプリントジョブを暗号化することを可能とする。

【０１６８】図８は、本発明に係る画像処理システムのデータ処理方法の第２実施例を示すフローチャートであり、外部装置であるホストコンピュータ２側のプリント時の制御手順に対応する。なお、（１）～（８）は各ステップを示す。

【０１６９】まず、ステップ（１）で第１実施例と同様にしてプリントすべきプリンタを選択する。次に、ステップ（２）でプリンタの変更を操作者が指定しているかどうかを判定し、指定していると判定された場合は、ステップ（１）に戻って再度プリンタの選択から繰り返す。

【０１７０】一方、ステップ（２）で変更がないと判定された場合は、ステップ（３）でプリント要求があるかどうか判定し、プリント要求がないと判定された場合は、ステップ（２）に戻る。

【０１７１】一方、ステップ（３）でプリント要求があると判定された場合は、ステップ（４）で暗号化が必要かどうかを操作者の指定、文書のセキュリティレベル等から判断し、暗号化が必要でないと判定された場合は、ステップ（７）に進むが、暗号化が必要であると判定された場合は、まず、ステップ（５）で選択されたプリンタの暗号化鍵をネットワーク４上に流れるデータからピックアップする。

【０１７２】本実施例においては、各プリンタの暗号化鍵はコンピュータから問い合わせる方式ではなく、一定時間毎にプリンタ側からネットワーク４上の全ての装置にブロードキャストする方式をとっている。

【０１７３】ステップ（５）では、このブロードキャストされた各プリンタの暗号化鍵の中から、ステップ（１）で選択されたプリンタの暗号化鍵をピックアップしてワークメモリ領域１０－２上に保持する。

【０１７４】ただし、必ずしもステップ（５）のみで待つ必要はなく、例えばステップ（１）で選択された後は、常にネットワーク４を監視していて、選択されたプリンタからブロードキャストされた暗号化鍵を拾い上げ、ワークメモリ領域１０－２上に記憶しておいてもいいし、また、ネットワーク４上にブロードキャストされた各プリンタの暗号化鍵を全て、または一定数拾い上げ、ワークメモリ領域１０－２上に記憶しておいてもよい。

【０１７５】さらに、各プリンタは個別暗号化鍵と、グループ別暗号化鍵の両方をブロードキャストするので、必要に応じ、どちらか、または両方ともピックアップするように構成してもよい。

【０１７６】本実施例の画像処理装置では、装置固有の暗号化鍵と復号化鍵とがあるタイミングで変化するような構成になっているため、プリント直前に暗号化鍵を獲得するようにしている。

【０１７７】次に、ステップ（６）において、まず、ホストコンピュータ自身の暗号化鍵ｊをプリントジョブに付加し、ステップ（５）でピックアップした暗号化鍵を用いて、ホストコンピュータ自身の暗号化鍵ｊを付加したプリントジョブを暗号化する。

【０１７８】第２実施例では、ホストコンピュータも自装置固有の暗号化鍵ｊと復号化鍵j^{-1}を持っている。また、ホストコンピュータ自身の暗号化鍵ｊを暗号化するのは、これを書き換えられないようにするためである。

【０１７９】そして、ステップ（７）では必要に応じて暗号化処理されたプリントジョブを暗号化に使用した暗号化鍵と共に、ステップ（１）で選択されたプリンタに送付する。ただし、暗号化を行わなかった場合は、暗号化鍵として「０」を送付する。また、暗号化鍵自体は暗号化せずに送付する。次いで、ステップ（８）では、認証応答タスク（後述する図９に示す処理）を起動し、ステップ（２）に戻る。

【０１８０】図９は、図８に示した認証応答タスクの詳細手順の一例を示すフローチャートである。なお、（１），（２）は各ステップを示す。

【０１８１】次に認証応答タスクは、ステップ（１）でプリンタからの認証要求を持ち、認証要求があれば、ステップ（２）で応答する。

【０１８２】なお、本実施例の場合は、認証要求とは、プリントジョブを作成したホストコンピュータとプリントジョブを送付したホストコンピュータが同一であるかどうかを確認するための試験であり、具体的に言えば、プリントジョブを受信したプリンタからテストデータＳ１が送られてくる。これに対し、プリントジョブを送信したホストコンピュータは、Ｓ２＝ｆ（j^{-1}（Ｓ１））の計算を行って、データＳ２をプリンタに送り返すことが要求される。

【０１８３】ここで、j^{-1}はプリントジョブを作成したホストコンピュータの復号化鍵であり、ｆはジョブを受信したプリンタの暗号化鍵である。ｆは一般には公開されているが、j^{-1}はプリントジョブを作成したホストコンピュータのみしか知らない。一方、データＳ２を受け取ったプリンタは、Ｓ３＝ｊ（f^{-1}（Ｓ２））の計算を行うことによりデータＳ３を得る。

【０１８４】ここで、f^{-1}はジョブを受信したプリンタの復号化鍵であり、ｊはプリントジョブを作成したホストコンピュータの暗号化鍵である。ｊはプリントジョブ中に含まれていて、また一般に公開されているが、f^{-1}はジョブを受信したプリンタのみしか知らない。この結果、プリントジョブを作成したホストコンピュータが、そのプリントジョブを送信して、認証要求にも応じた場合は、

Ｓ３＝ｊ（f^{-1}（Ｓ２）＝ｊ（f^{-1}（ｆ（j^{-1}（Ｓ１））））＝ｊ（j^{-1}（Ｓ１））＝Ｓ１

となり、データＳ１とデータＳ３が一致する。

【０１８５】一方、プリントジョブを作成したホストコンピュータとプリントジョブを送信したホストコンピュータが異なる場合は、後者はj^{-1}を知らないため、正しいデータＳ２を返せない。よってデータＳ１とデータＳ３が一致しない。

【０１８６】以上は、プリントジョブを作成したホストコンピュータとプリントジョブを送信したホストコンピュータが異なる場合はプリントしないようにするための仕組みである。この仕組みは、あるホストコンピュータが作成し、あるプリンタに送信したプリントジョブが、ネットワーク転送中に別のコンピュータに盗まれ、後日、盗んだコンピュータが同じプリンタに送信してプリントすることを防ぐためのものである。

【０１８７】図１０は、図２に示した画像処理装置による第２のメインタスクの一例を示すフローチャートである。なお、（１）～（６）は各ステップを示す。

【０１８８】まず、図１０のメインタスクでは、電源オン後、ステップ（１）でプリントキューＰＣに以前に受信した暗号化されたプリントジョブが残っているのか判断し、残っていなければステップ（２）で、その装置個別の暗号化鍵と復号化鍵を別のものに変更する。これは画像処理装置内のプログラムの解析等により復号化鍵が万一盗まれた場合に対する処理であり、また、あるタイミングで復号化鍵を変更することにより盗まれにくくするためのものである。

【０１８９】ステップ（１）で以前に受信した暗号化されたプリントジョブが残っている場合は、復号化鍵を変更すると復号化できなくなるため、変更はしない。

【０１９０】次にステップ（３）で受信タスクを起動し、ステップ（４）でプリントタスク（後述する図１１参照）を起動する。次いで、ステップ（５）でネットワークに接続されている各装置にネットワーク経由で、自装置の個別暗号化鍵とグループ別暗号化鍵をブロードキャストする。そして、ステップ（６）で一定時間待った後、ステップ（５）に戻りブロードキャストを繰り返す。

【０１９１】第２の実施例の画像処理装置３の受信タスクは、第１実施例とほぼ同じであるので図６を用いて違いを説明する。

【０１９２】まず、第２実施例では、暗号化鍵はブロードキャストにより外部装置に公開されるので、ステップ（１），ステップ（２）の処理がない。

【０１９３】次に、ステップ（３），ステップ（４），ステップ（６）の処理は第１実施例と同じであるが、ステップ（５）において、暗号化されたプリントジョブの行き先としてホールドキューが指定された場合には、ホールドキューＨＣに入れずに、すぐに削除してしまうところが異なっている。

【０１９４】これは暗号化されたジョブをホールドキューに保持しておくのは、他人に後でプリントキューＰＣに移動され、プリントされる危険性があるのを防ぐためである。もちろん、暗号化されたジョブはパスワードなどを入力しないと移動できない構成にしておけば、第１実施例のように、ホールドキューＨＣや完了キューＥＣに暗号化されたジョブを保持するようにしても危険は少ない。

【０１９５】図１１は、図２に示した画像処理装置による第２のプリントタスクの一例を示すフローチャートである。なお、（１）～（１３）は各ステップを示す。

【０１９６】本実施例のプリントタスクでは、まず、ステップ（１）でプリントキューの先頭のジョブをピックアップする。ステップ（２）ではピックアップしたジョブが、暗号化されていないか、暗号化されている場合は、どの暗号化鍵で暗号化されているかを、ジョブに付加された暗号化鍵で判断する。

【０１９７】まず、ステップ（２）でジョブに付加された暗号化鍵（内容「０」）が暗号化していないことを意味する場合は、ステップ（１１）で、そのジョブの各ページを順次、フルページ画像メモリ１０－１上に展開し、ステップ（１２）で展開した画像データを画像形成装置１に送ってプリントを行う。全てのページをプリント後、ステップ（１３）でプリント終了したジョブを完了キューＥＣに移動し、ステップ（１）に戻る。

【０１９８】一方、ステップ（２）で、自装置の個別暗号化鍵とジョブに付加された暗号化鍵が一致した場合は、ステップ（３）で自装置の個別暗号化鍵に対応した個別復号化鍵を準備し、ステップ（５）に移る。

【０１９９】一方、ステップ（２）で自装置のグループ別暗号化鍵とジョブに付加された暗号化鍵が一致した場合は、ステップ（４）で自装置のグループ別暗号化鍵に対応したグループ別復号化鍵を準備し、ステップ（５）に移る。

【０２００】一方、ステップ（２）で自装置の個別暗号化鍵とも、グループ別暗号化鍵とも、ジョブに付加された暗号化鍵が一致しない場合は、図１１には記述していないが、そのジョブを削除してステップ（１）に戻る。

【０２０１】次に、ステップ（５）では、ステップ（３）、またはステップ（４）で準備された復号化鍵を用いて復号化しつつ、そのジョブの各ページを順次、フルページ画像メモリ１０－１上に展開する。次に、ステップ（６），ステップ（７）では、プリントジョブを送信してきたホストコンピュータがプリントジョブを作成したホストコンピュータと同一であるかの認証を行う。

【０２０２】具体的には、まず、ステップ（６）でテストデータＳ１を、プリントジョブを送信してきたホストコンピュータに送る。次いで、ホストコンピュータから、前述の演算されたデータＳ２が送り返されてくるので、ステップ（７）でＳ３＝ｊ（f^{-1}（Ｓ２））を計算し、データＳ１とデータＳ３が一致するかどうかを確認する。この場合の、ｊはステップ（５）で復号化されたジョブ内に含まれるプリントジョブを作成したホストコンピュータの暗号化鍵である。

【０２０３】ステップ（７）でデータＳ１とデータＳ３が上記一致しないと判定された場合は、プリントジョブを送信してきたホストコンピュータがプリントジョブを作成したホストコンピュータと同一でないので、ステップ（８）でジョブを削除し、画像メモリ内の情報をクリアしてステップ（１）に戻る。

【０２０４】一方、ステップ（７）でデータＳ１とデータＳ３が一致したと判定された場合は、ステップ（９）で、展開した画像データを画像形成装置１に送ってプリントを行う。図１１には記載していないが、ステップ（５）からステップ（９）までの処理を、そのジョブの各ページについて順次行う。全てのページをプリント後、ステップ（１０）でプリント終了したジョブを削除し、画像メモリ内の情報をクリアしてステップ（１）に戻る。

【０２０５】このように第２実施例の場合は、暗号化されたジョブは完了キューＥＣには移動しない。

【０２０６】本実施例では、暗号化されたプリントジョブはホールドキューＨＣや完了キューＥＣに入れないようにしたが、これを入れるようにし、逆に暗号化されたプリントジョブはホールドキューＨＣや完了キューＥＣからプリントキューＰＣに移動できないように構成してもよい。この構成でも、実質的に、ホールドキューＨＣや完了キューＥＣに入れられたプリントジョブはプリントされることなく、削除のみ可能となるので本実施例の構成と同じ効果となる。

【０２０７】上記実施例では、プリントジョブを復号化した後、プリント直前にホストコンピュータの認証を行っている。これは、プリントジョブを作成したホストコンピュータの暗号化鍵が書き換えられないように暗号化されているため、それを復号化した後、認証を行うようにしたものであり、これによって復号化が１回で済ませることができるわけである。

【０２０８】一方、その代わりに、プリントジョブを受信した直後に、プリントジョブの一部を復号化してホストコンピュータの暗号化鍵を獲得し、直ちに、認証を行うようにした構成も一つの実施例である。この場合は、復号化を２回しなければならないが、プリントジョブの受信直後に、認証を行え、認証が終わったら直ちにホストコンピュータとの通信を終了できるという特徴がある。

【０２０９】即ち、ホストコンピュータ側は図９に示す認証応答タスクを起動して認証処理を待つことなく、図８のステップ（８）の時点で直ちに認証を行える。また、認証を行うための情報が暗号化されていない場合は、復号化を待つ必要がないため、プリントジョブを受信した直後に認証を行う構成の方が好ましい。

【０２１０】〔第３実施例〕上記第２実施例では、プリントジョブを送信してきたホストコンピュータがプリントジョブを作成したホストコンピュータと同一であるかの認証を行う場合について説明したが、プリントジョブを送信してきたホストコンピュータがプリンタにあらかじめ登録されているホストコンピュータかどうかの認証を行うように構成してもよい。以下、その実施例について説明する。

【０２１１】なお、第２の実施例と同様な部分については説明を省略し、第２の実施例と異なる部分についての

み説明する。

【0212】第1に、第3の実施例のホストコンピュータ側のプリント処理では、プリントジョブにホスト側暗号化鍵jを付加する代わりに、任意のデータS1，データS2（S2＝f（j^{-1}（S1））を付加する。ここで、j^{-1}はプリントジョブを作成したホストコンピュータの復号化鍵であり、fはジョブを受信するプリンタの暗号化鍵である。

【0213】第2に、第3実施例の画像処理装置側のプリント処理では、図11のステップ（6）の認証要求において、まず、プリントジョブを送信してきたホストコンピュータがあらかじめ登録されているホストコンピュータかどうかの確認を行う。これは、送信してきたホストコンピュータの名前が、プリンタに登録（例えば図示しないNVRAMまたはハードディスク8等に記憶される）されているリストに入っているかどうかで判断し、入っていないと判断された場合、ステップ（8）に移り、プリントしない。

【0214】一方、ステップ（6）において、入っていると判断された場合は、そのリストから、そのホストコンピュータの公開されている暗号化鍵kを獲得する。次に、S3＝k（f^{-1}（S2））の計算を行うことによりデータS3を得る。ここで、送信してきたホストコンピュータが、あらかじめ登録されているホストコンピュータである場合には、j＝kとなるので、S3＝k（f^{-1}（S2））＝k（f^{-1}（f（j^{-1}（S1））））＝k（j^{-1}（S1））＝S1となり、データS1とデータS3が一致することとなる。

【0215】一方、送信してきたホストコンピュータが、別の登録されているコンピュータの名前を使っていた場合は、j^{-1}を知らないため、正しいデータS2を作れず、データS1とデータS3が一致しない。この場合は、ステップ（8）に移り、プリントしない。

【0216】これにより、プリンタに登録されているホストコンピュータ以外からはプリントできない仕組みを提供することができる。

【0217】なお、第3の実施例においては、公開鍵暗号方式を用いて、プリントジョブを送信してきたホストコンピュータがあらかじめ登録されているホストコンピュータかどうかの認証を行うようにしたものであり、安全性が高いという特徴を持つが、これをもっと簡単な処理で認証するように構成してもよい。

【0218】例えばプリントジョブの中にホストコンピュータ名を入れて、それがあらかじめ登録されているホストコンピュータ名かどうかのチェックを行い、簡単な処理で認証処理を行えるように構成してもよい。

【0219】本実施例においては、プリンタに登録されているホストコンピュータ以外からはプリントできないようにしているが、これを例えば、登録されているプリンタについても登録内容に応じてモードを制限するようにしたり、プリント枚数、使用時間を制限するようにした構成も、その条件でプリントできるように登録されていないのと等価であるため、その点においては本実施例と同等の効果を期待できる。

【0220】〔他の実施例〕上記の各実施例では、ホストコンピュータから受け取る画像データをPDLデータの形式で受け取っていた。この形式は、文字データ，図形データ，ラスタ画像データを統一的に扱えるという特徴を持っている。また、ラスタ画像データのみの画像データ等と比べて、一般にデータ量が少ないので、暗号化処理や復号化処理に時間がかからないという特徴を持っている。

【0221】しかし、このPDLデータの代わりに、ラスタ画像データのみを受け取り、それを画像メモリに書き込むという場合も1つの実施例である。この場合は、複雑な展開処理を行わないため、CPU，ROM，RAM等について高速なものを使う必要がなく、価格を安くできるという特徴がある。

【0222】また、上記の各実施例では、暗号化処理、復号化処理をソフトウェアで行っているが、これをハードウェアで行ってもよい。

【0223】さらに、上記の各実施例では、ラスタ画像データをそのまま画像メモリ上に展開したり、スプール用ハードディスクに保持していた。これはハード構造を簡単にできるという特徴を持っている。

【0224】しかし、そのまま展開する代わりに、何等かの圧縮を施して画像メモリやスプール用ハードディスクに保持するようにした場合も1つの実施例である。この場合は、ハード構造は複雑になるが、メモリ量を減らせるという効果がある。

【0225】また、各実施例においては、外部のホストコンピュータ等から通信により、PDLデータ等の画像データを受け取っていたが、これを内部のフロッピーディスクから画像データを読み取るようにした場合も1つの実施例である。

【0226】また、フロッピーディスクの代わりにハードディスク等でも良く、また、図示しないアプリケーションプログラムで作られたPDLデータをメインメモリ上で、受け渡してもよい。

【0227】また、上記の各実施例では、画像形成装置1－1，1－2は、画像処理装置3－1，3－2と分離しているが、これを一体化しても良い。

【0228】さらに、上記の各実施例ではローカルエリアネットワークを用いているが、これを都市間や国家間をまたいで接続するワイドエリアネットワークを用いるようにしてもよい。

【0229】また、上記の各実施例では、プリントジョブ全体を公開された暗号化鍵で暗号化する場合について説明したが、これをプリントジョブ全体を任意の第2の暗号化鍵で暗号化し、その第2の暗号化鍵自体を公開さ

れた暗号化鍵で暗号化し、暗号化されたプリントジョブに加えて、暗号化された暗号化鍵をプリンタに送付して、すなわち、第２の暗号化鍵による暗号化手法として比較的処理の軽い暗号化手法を用いることにより、プリントジョブ全体の暗号化／復号化を比較的短時間で処理でき、しかも公開鍵暗号方式の利点が残るように構成してもよい。

【０２３０】さらに上記の各実施例では、ＲＳＡ暗号に代表される公開鍵暗号方式の暗号化鍵、復号化鍵を用いている場合について説明したが、装置固有の同一の暗号化鍵を、複数の外部装置に公開する暗号方式であれば、多少安全性が低くても本発明を適用可能となる。例えば、暗号化鍵から復号化鍵を、比較的短時間で求められるような場合でも、暗号化を行わない場合よりは安全性が向上する。

【０２３１】なお、本発明は、複数の機器から構成されるシステムに適用しても、１つの機器からなる装置に適用してもよい。また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適用できることは言うまでもない。この場合、本発明を達成するためのソフトウェアによって表されるプログラムを格納した記憶媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０２３２】さらに、本発明を達成するためのソフトウェアによって表されるプログラムをネットワーク上のデータベースから通信プログラムによりダウンロードして読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０２３３】

【発明の効果】以上説明したように、本発明に係る第１の発明によれば、通知手段による前記プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知後、プリントジョブ受信手段が前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信したら、復号手段が受信した暗号化されたプリントジョブを前記記憶手段に記憶された前記復号化鍵情報に基づいて復号化し、展開手段が該復号化したプリントジョブ中の各ページの画像データを画像メモリ上に展開するので、通信媒体上に出力された該プリントジョブは該暗号化鍵情報を提示した画像処理装置以外の画像処理装置では実質上復号化不能とした状態で転送し、該暗号化鍵情報を復号可能な画像処理装置の復号化鍵情報に基づいて画像出力可能なプリントジョブに復号してプリントジョブを処理することができる。

【０２３４】第２の発明によれば、前記通知手段は、同一の暗号化鍵情報を前記通信媒体を介して各情報処理装置に通知して、プリントジョブを暗号化するための暗号化鍵情報を全ての情報処理装置に対して共通化することを可能とする。

【０２３５】第３の発明によれば、所定のネットワークを介して暗号化鍵情報を複数の情報処理装置に通知して、各情報処理装置に通知した暗号化鍵情報を容易に変更することができる。

【０２３６】第４の発明によれば、復号手段は、前記展開手段による画像データの展開の直前、もしくは展開中に前記受信した暗号化されたプリントジョブの復号を行い、暗号化されたプリントジョブ全体が復号化されてしまう事態を回避することができる。

【０２３７】第５の発明によれば、暗号化鍵情報に対する前記復号化鍵情報との組合せを複数備え、他の画像処理装置と共有してあるいは各画像処理装置固有にプリントジョブを暗号化／復号化する異なる環境を共存させることができる。

【０２３８】第６の発明によれば、第１の制御手段は前記プリントジョブに付加された有効期限情報に基づいて受信したプリントジョブの処理を制御するので、暗号化されたプリントジョブが転送中に第３者により入手されてしまっても、有効期限情報の制約に合致しない場合には、復号化できたプリントジョブであってもその画像出力を確実に制限することができる。

【０２３９】第７の発明によれば、有効期限情報は、暗号化された状態で前記プリントジョブに付加するので、有効期限情報の書き換えを防止することができる。

【０２４０】第８の発明によれば、認証手段により受信したプリントジョブを作成した情報処理装置と受信したプリントジョブを送信した情報処理装置とが同一であるかを認証し、該認証結果に基づいて第２の制御手段が受信したプリントジョブの処理を制御するので、いずれかの情報処理装置が通知された暗号化鍵情報に基づいて暗号化されたプリントジョブを他の情報処理装置が取得する事態が発生しても、該他の情報処理装置から取得したプリントジョブを対応する画像処理装置から出力されてしまう事態を確実に制限することができる。

【０２４１】第９の発明によれば、プリントジョブ受信手段は、前記暗号化鍵情報により暗号化されたプリントジョブおよび暗号化鍵情報を併せて各情報処理装置から受信して、受信したプリントジョブの暗号化状態を確実に識別するので、対応する最適な復号化鍵情報に基づいて受信したプリントジョブを正常に復号化することができる。

【０２４２】第１０の発明によれば、プリントジョブ受信手段が各情報処理装置から受信する暗号化鍵情報は暗号化されていない状態で受信するので、受信した暗号化鍵情報と通知した暗号化鍵情報とから暗号化に使用された暗号化鍵情報を確実に識別することができる。

【０２４３】第１１の発明によれば、第１の保持手段が前記暗号化鍵情報により暗号化されたプリントジョブを印刷候補として複数一時的に保持するので、印刷候補となるプリントジョブ自体は印刷される直前まで暗号化さ

れた状態で保持することができる。

【０２４４】第１２の発明によれば、第２の保持手段が前記暗号化鍵情報により暗号化されたプリントジョブを出力待機候補として複数一時的にそのまま保持するので、出力待機状態となっているプリントジョブ自体は印刷される直前まで暗号化された状態で保持することができる。

【０２４５】第１３の発明によれば、前記展開手段により画像メモリ上に展開された画像データが送出手段により画像出力装置に送出されて、前記画像出力装置による画像出力が完了したら、第３の保持手段が前記暗号化鍵情報により暗号化されたプリントジョブを破棄候補として複数一時的に保持するので、復号化されて画像出力装置から出力されてしまったプリントジョブがそのままの状態で保持されてしまうことを回避することができる。

【０２４６】第１４の発明によれば、前記展開手段により画像メモリ上に展開された画像データが送出手段により画像出力装置に送出されて、前記画像出力装置による画像出力が完了したら、第３の保持手段が前記暗号化鍵情報により暗号化されていないプリントジョブを破棄候補として複数一時的に保持するので、画像出力が完了している暗号化されていたプリントジョブが不用意に保持される状態を回避することができる。

【０２４７】第１５の発明によれば、前記暗号化されたプリントジョブは、所定のページ記述言語で記述された印刷情報を暗号化鍵情報に基づいて暗号化するので、ページ記述言語中で容易に可読できるデータを確実に暗号化して転送処理することができる。

【０２４８】第１６の発明によれば、前記暗号化鍵情報と対となる復号化鍵情報は、所定の公開鍵暗号方式に準拠するので、プリントジョブの暗号化／復号化処理環境を容易に構築することができる。

【０２４９】第１７の発明によれば、暗号受信手段がいずれかの画像処理装置から所定の暗号化鍵情報を受信したら、該受信された前記所定の暗号化鍵情報に基づいて暗号化手段が作成されたプリントジョブを暗号化し、該暗号化されたプリントジョブをプリントジョブ送信手段が前記所定の暗号化鍵情報を受信した画像処理装置に送信するので、いずれの情報処理装置に対しても同一の暗号化鍵情報で通知して暗号化されたプリントジョブの復号化処理を画一化することができる。

【０２５０】第１８の発明によれば、第１の暗号化鍵情報記憶手段が前記暗号受信手段により前記所定の通信媒体を介して各画像処理装置から受信した固有の暗号化鍵情報を記憶するので、いずれの画像処理装置に対しても対応する暗号化鍵情報に基づいて暗号化されたプリントジョブを転送することができる。

【０２５１】第１９の発明によれば、暗号受信手段は、前記暗号化手段による暗号化開始直前に各画像処理装置から前記固有の暗号化鍵情報を受信するので、各画像処理装置が通知する暗号化鍵情報が変更されても、常に復号可能となる最新の暗号化鍵情報に基づいてプリントジョブを暗号化することができる。

【０２５２】第２０の発明によれば、第２の暗号化鍵情報記憶手段は前記暗号受信手段により前記所定の通信媒体を介して各画像処理装置から受信した複数の画像処理装置で共通する暗号化鍵情報を記憶するので、いずれの画像処理装置に対しても対応する暗号化鍵情報に基づいて暗号化されたプリントジョブをグループ化されたいずれかの画像処理装置に転送することができる。

【０２５３】第２１の発明によれば、前記暗号受信手段は、前記暗号化手段による暗号化開始直前に複数の画像処理装置で共通する暗号化鍵情報各を受信するので、複数の画像処理装置が通知する暗号化鍵情報が変更されても、常に復号可能となる最新の暗号化鍵情報に基づいてプリントジョブを暗号化することができる。

【０２５４】第２２の発明によれば、プリントジョブは、画像処理装置における画像処理実行状態を制御するための所定の有効期限情報を含むので、暗号化されたプリントジョブが画像処理装置側で復号化されても、有効期限外であれば当該プリントジョブの出力を制限することができる。

【０２５５】第２３の発明によれば、暗号化手段は、画像処理装置における画像処理実行状態を制御するための所定の有効期限情報を含むプリントジョブを暗号化するので、有効期限外であれば当該プリントジョブの出力を制限するための有効期限情報が容易に解読されてしまうことを防止することができる。

【０２５６】第２４の発明によれば、前記プリントジョブ送信手段は、前記暗号化手段により暗号化されたプリントジョブおよび前記暗号化手段が暗号化に使用した前記所定の暗号化鍵情報も同時に画像処理装置に送信するので、暗号化されたプリントジョブを受信する画像処理装置が当該暗号化鍵情報を識別することができる。

【０２５７】第２５の発明によれば、前記プリントジョブ送信手段は、前記暗号化手段が暗号化に使用した前記所定の暗号化鍵情報をそのまま画像処理装置に送信するので、暗号化されたプリントジョブを受信する画像処理装置が当該暗号化鍵情報が識別不能となる事態を回避することができる。

【０２５８】第２６の発明によれば、通知手段による前記プリントジョブを暗号化するための暗号化鍵情報が各情報処理装置に通知されると、暗号受信手段がいずれかの画像処理装置から所定の暗号化鍵情報を受信し、該受信された前記所定の暗号化鍵情報に基づいて暗号化手段が作成されたプリントジョブを暗号化し、該暗号化されたプリントジョブをプリントジョブ送信手段が前記所定の暗号化鍵情報を受信した画像処理装置に送信し、プリントジョブ受信手段が前記暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信したら、

復号手段が受信した暗号化されたプリントジョブを前記記憶手段に記憶された前記復号化鍵情報に基づいて復号化し、展開手段が該復号化したプリントジョブ中の各ページの画像データを画像メモリ上に展開するので、いずれの情報処理装置に対しても同一の暗号化鍵情報で通知して暗号化されたプリントジョブの復号化処理を画一化し、かつ通信媒体上に出力された該プリントジョブは該暗号化鍵情報を提示した画像処理装置以外の画像処理装置では実質上復号化不能とした状態で転送し、該暗号化鍵情報を復号可能な画像処理装置の復号化鍵情報に基づいて画像出力可能なプリントジョブに復号してプリントジョブを処理することができる。

【０２５９】第２７の発明によれば、いずれかの画像処理装置から所定の暗号化鍵情報を受信し、該受信された前記所定の暗号化鍵情報に基づいて作成されたプリントジョブを暗号化し、該暗号化されたプリントジョブを前記所定の暗号化鍵情報を受信した画像処理装置に送信するプリントジョブ送信するので、いずれの情報処理装置に対しても同一の暗号化鍵情報で通知して暗号化されたプリントジョブの復号化処理を画一化する処理を自動化することができる。

【０２６０】第２８の発明によれば、プリントジョブを暗号化するための暗号化鍵情報を各情報処理装置に通知し、該通知された暗号化鍵情報により暗号化されたプリントジョブを各情報処理装置から受信し、該受信したプリントジョブを前記復号化鍵情報に基づいて復号化し、該復号化したプリントジョブに基づいてプリントジョブ中の各ページの画像データを画像メモリ上に展開するので、通信媒体上に出力された該プリントジョブは該暗号化鍵情報を提示した画像処理装置以外の画像処理装置では実質上復号化不能とした状態で転送し、該暗号化鍵情報を復号可能な画像処理装置の復号化鍵情報に基づいて画像出力可能なプリントジョブに復号する処理を自動化することができる。

【０２６１】従って、通信媒体上のプリントジョブを容易に暗号化し、かつ、画像処理装置以外は暗号化されたプリントジョブを実質上復号化できない機密保持性に優れたプリントジョブ処理環境を構築することができる等の効果を奏する。

【図面の簡単な説明】

＊【図１】本発明の第１の実施例を示す画像処理システムの構成を説明する概略ブロック図である。

【図２】図１に示した画像処理装置と画像形成装置とから構成される画像処理システムの要部構成を説明するブロック図である。

【図３】図１に示したコンピュータと画像処理装置との間におけるプリントジョブの暗号化／複合化処理状態を説明する模式図である。

【図４】図２に示したハードディスクのスプール領域に配置される待ち行列を説明するための図である。

【図５】本発明に係る画像処理システムのデータ処理方法の第１実施例を示すフローチャートである。

【図６】本発明に係る画像処理システムのデータ処理方法の第１実施例を示すフローチャートである。

【図７】図２に示した画像処理装置による第１のプリントタスクの一例を示すフローチャートである。

【図８】本発明に係る画像処理システムのデータ処理方法の第２実施例を示すフローチャートである。

【図９】図８に示した認証応答タスクの詳細手順の一例を示すフローチャートである。

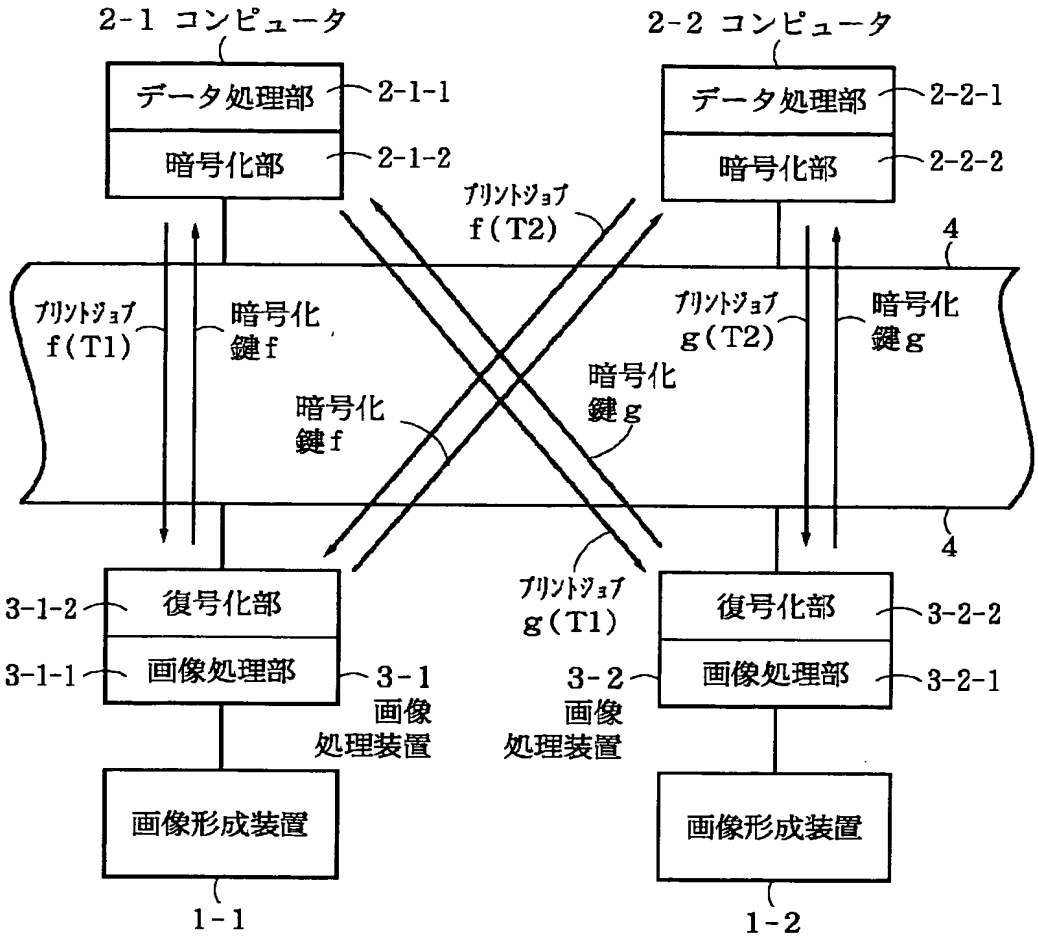
【図１０】図２に示した画像処理装置による第２のメインタスクの一例を示すフローチャートである。

【図１１】図２に示した画像処理装置による第２のプリントタスクの一例を示すフローチャートである。

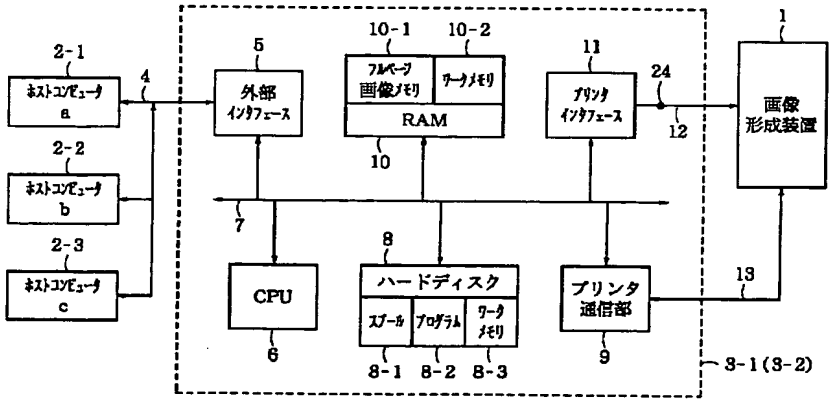
【符号の説明】

１－１　画像形成装置
１－２　画像形成装置
２－１　情報処理装置（コンピュータ）
２－２　情報処理装置（コンピュータ）
２－１－１　データ処理部
２－１－２　暗号化部
２－２－１　データ処理部
２－２－２　暗号化部
３－１　画像処理装置
３－２　画像処理装置
３－１－１　画像処理部
３－１－２　復号化部
３－２－１　画像処理部
３－２－２　復号化部

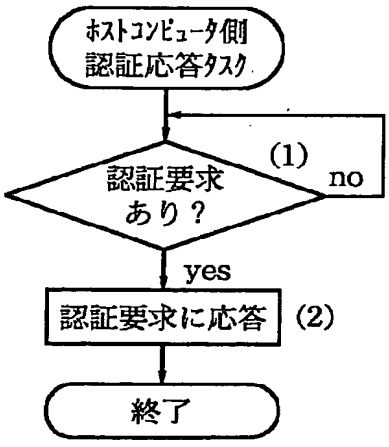
【図１】


2-1 コンピュータ
2-2 コンピュータ
データ処理部
2-1-1
暗号化部
2-1-2
データ処理部
2-2-1
暗号化部
2-2-2
プリントジョブ
f(T2)
4
プリントジョブ
f(T1)
暗号化
鍵f
暗号化
鍵f
暗号化
鍵g
プリントジョブ
g(T2)
暗号化
鍵g
4
3-1-2
復号化部
3-1-1
画像処理部
3-1
画像
処理装置
プリントジョブ
g(T1)
復号化部
3-2-2
3-2
画像
処理装置
画像処理部
3-2-1
画像形成装置
画像形成装置
1-1
1-2

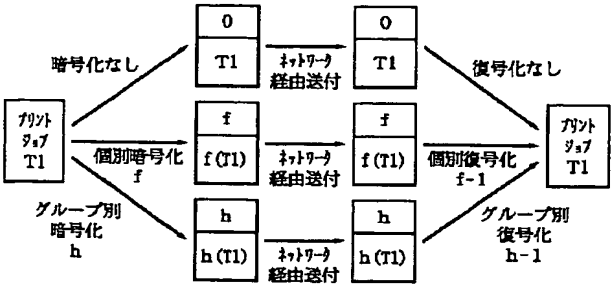
【図２】


2-1
ホストコンピュータ
a
2-2
ホストコンピュータ
b
2-3
ホストコンピュータ
c
4
5
外部
インタフェース
10-1
フルページ
画像メモリ
10-2
ワークメモリ
RAM
10
11
プリンタ
インタフェース
24
12
1
画像
形成装置
7
8
CPU
6
ハードディスク
スプール
プログラム
ワーク
メモリ
8-1
8-2
8-3
プリンタ
通信部
9
13
3-1(3-2)

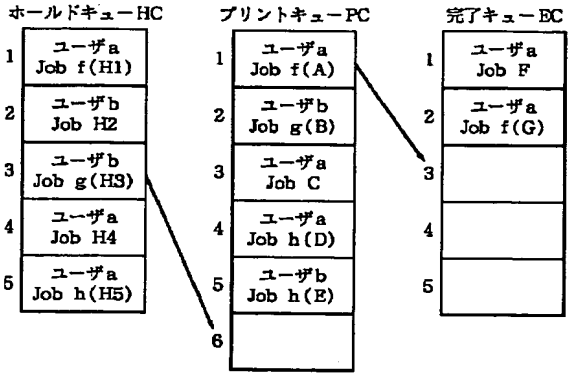
【図９】


ホストコンピュータ側
認証応答タスク
(1)
認証要求
あり？
no
yes
認証要求に応答
(2)
終了

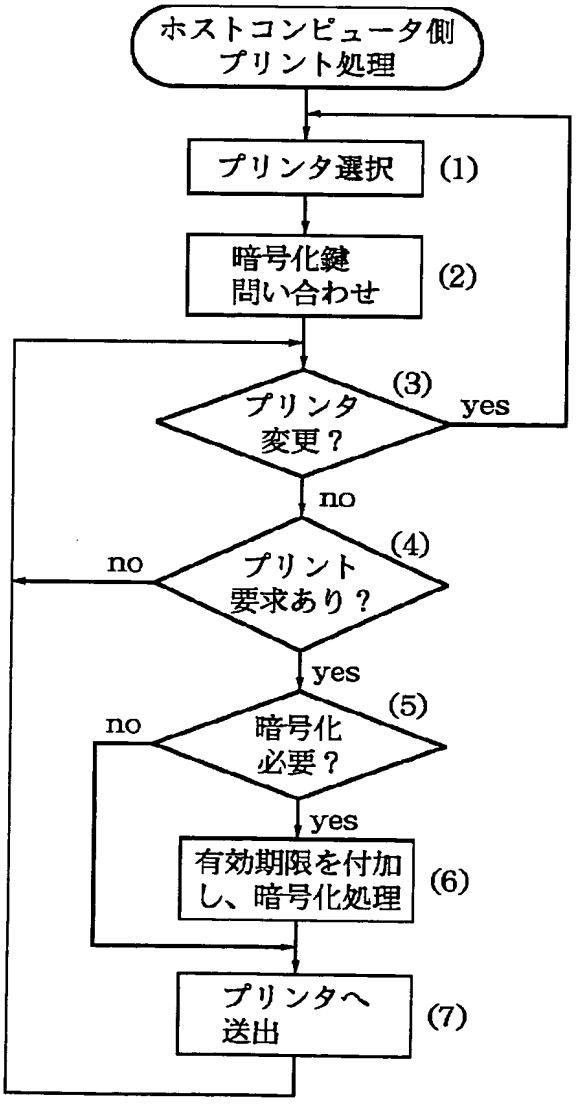
【図３】


プリントジョブ T1
暗号化なし
個別暗号化 f
グループ別暗号化 h
0
T1
f
f(T1)
h
h(T1)
ネットワーク経由送付
復号化なし
個別復号化 f-1
グループ別復号化 h-1

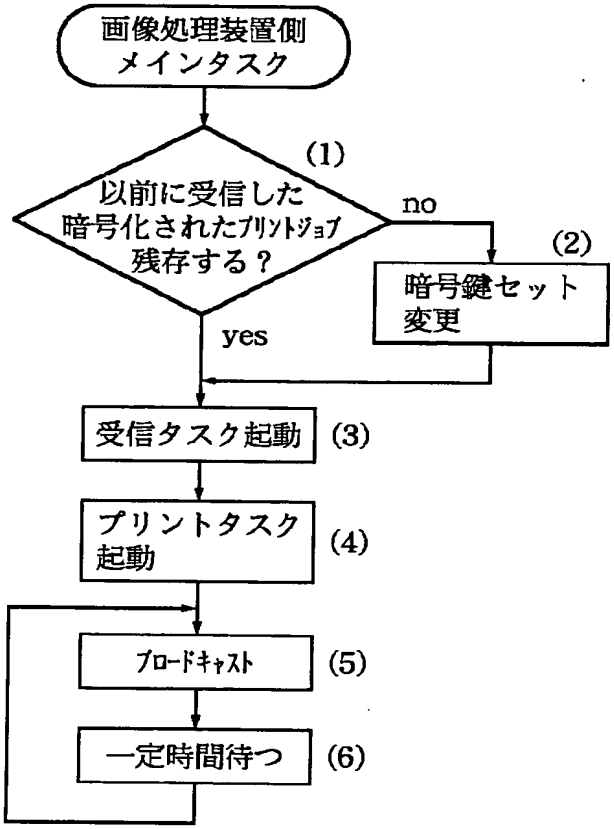
【図４】


ホールドキューHC
プリントキューPC
完了キューEC
ユーザa Job f(H1)
ユーザb Job H2
ユーザb Job g(H3)
ユーザa Job H4
ユーザa Job h(H5)
ユーザa Job f(A)
ユーザb Job g(B)
ユーザa Job C
ユーザa Job h(D)
ユーザb Job h(E)
ユーザa Job F
ユーザa Job f(G)

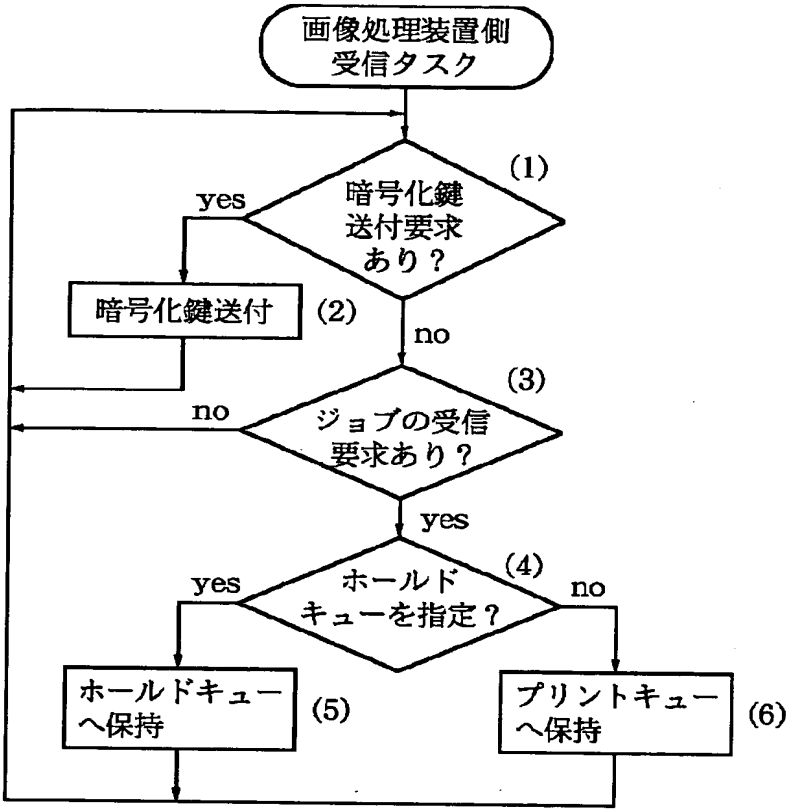
【図５】


ホストコンピュータ側 プリント処理
プリンタ選択 (1)
暗号化鍵 問い合わせ (2)
プリンタ 変更？ (3)
yes
no
プリント 要求あり？ (4)
no
yes
暗号化 必要？ (5)
no
yes
有効期限を付加し、暗号化処理 (6)
プリンタへ 送出 (7)

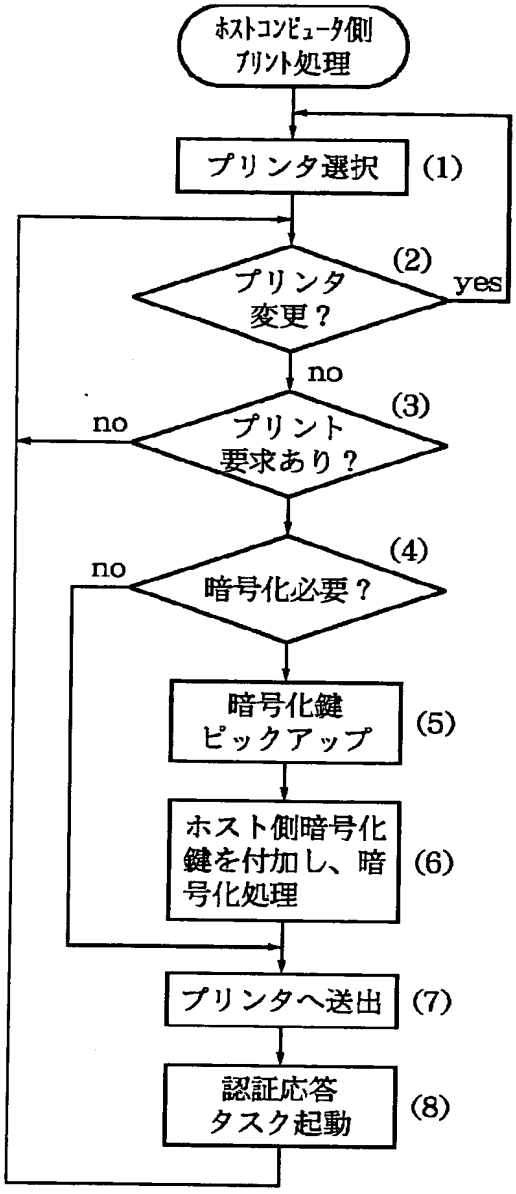
【図１０】


画像処理装置側 メインタスク
(1)
以前に受信した 暗号化されたプリントジョブ 残存する？
no
(2)
暗号鍵セット 変更
yes
受信タスク起動 (3)
プリントタスク 起動 (4)
ブロードキャスト (5)
一定時間待つ (6)

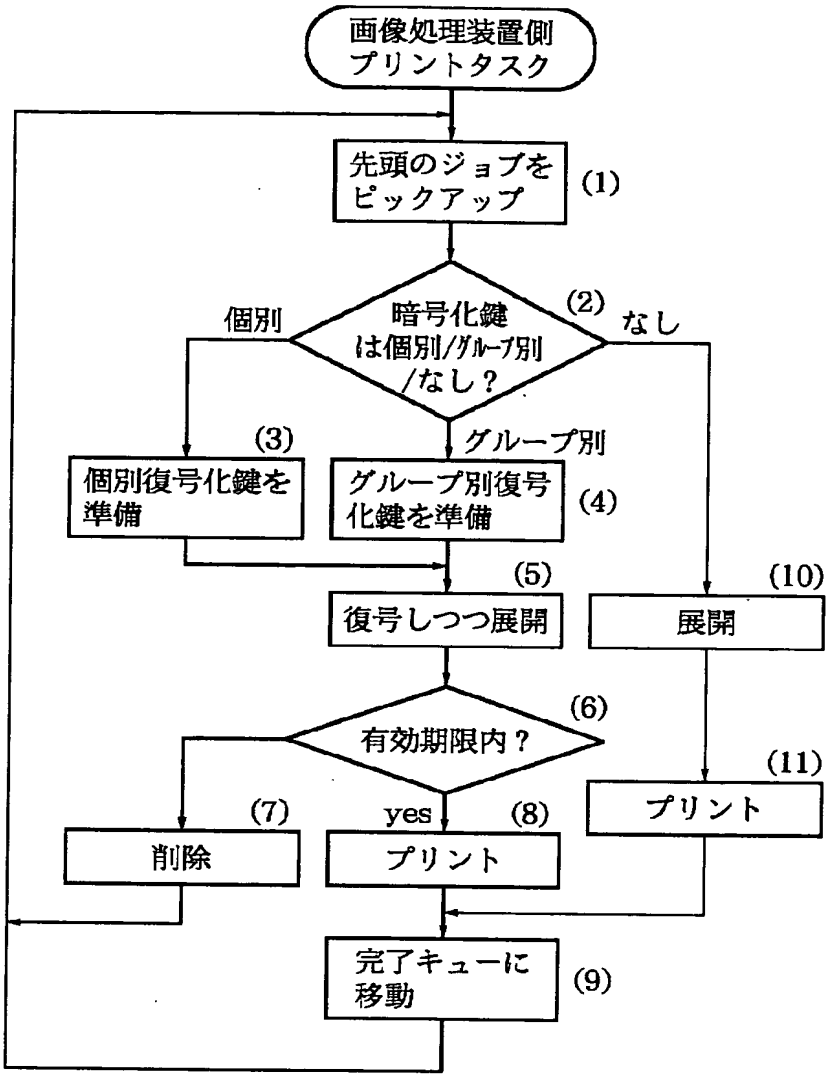
【図６】


画像処理装置側
受信タスク
暗号化鍵
送付要求
あり？
(1)
yes
no
暗号化鍵送付
(2)
ジョブの受信
要求あり？
(3)
no
yes
ホールド
キューを指定？
(4)
yes
no
ホールドキュー
へ保持
(5)
プリントキュー
へ保持
(6)

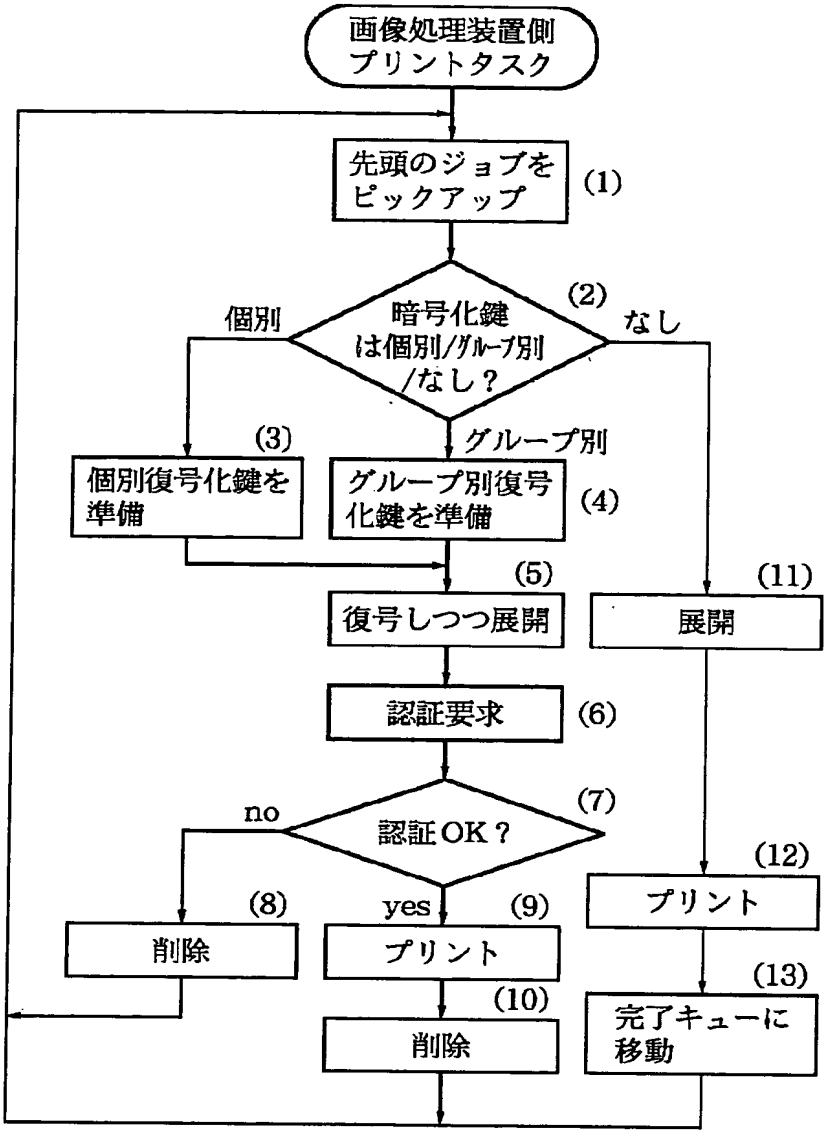
【図８】


ﾎｽﾄｺﾝﾋﾟｭｰﾀ側
ﾌﾟﾘﾝﾄ処理
プリンタ選択
(1)
プリンタ
変更？
(2)
yes
no
プリント
要求あり？
(3)
no
暗号化必要？
(4)
no
暗号化鍵
ピックアップ
(5)
ホスト側暗号化
鍵を付加し、暗
号化処理
(6)
プリンタへ送出
(7)
認証応答
タスク起動
(8)

【図７】


画像処理装置側
プリントタスク
先頭のジョブを
ピックアップ
(1)
暗号化鍵
は個別/ｸﾞﾙｰﾌﾟ別
/なし？
(2)
個別
なし
グループ別
(3)
個別復号化鍵を
準備
グループ別復号
化鍵を準備
(4)
(5)
復号しつつ展開
(10)
展開
有効期限内？
(6)
(11)
プリント
(7)
削除
yes
(8)
プリント
完了キューに
移動
(9)

【図１１】



フロントページの続き

(51) Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｇ０９Ｃ	1/00	６２０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６２０Ｂ	
Ｈ０４Ｌ	9/30			Ｈ０４Ｌ	9/00	６６３Ｂ	